CA ARCserve® Central Host-Based VM Backup

Guida per l'utente

r16.5

Riferimenti ai prodotti CA Technologies

Questo documento è valido per i seguenti prodotti di CA Technologies:

- CA ARCserve® Backup
- CA ARCserve® D2D
- CA ARCserve® Replication e High Availability
- CA ARCserve® Central Host-Based VM Backup
- CA ARCserve® Central Protection Manager
- CA ARCserve® Central Reporting
- CA ARCserve® Central Virtual Standby

Contattare il servizio di Supporto tecnico

Per l'assistenza tecnica in linea e un elenco completo delle sedi, degli orari del servizio di assistenza e dei numeri di telefono, contattare il Supporto tecnico visitando il sito Web all'indirizzo http://www.ca.com/worldwide.

Collegamenti di supporto per CA ARCserve Central Applications:

CA Support Online offre un insieme di risorse per la risoluzione di problemi tecnici e fornisce l'accesso a informazioni di prodotto importanti. Il CA Support consente di accedere facilmente a fonti di supporto disponibili in qualunque momento. I seguenti collegamenti consentono l'accesso a vari siti di CA Support disponibili per l'utente:

- **Informazioni sul Supporto tecnico** - Questo collegamento fornisce informazioni sui programmi di manutenzione e le offerte di supporto, inclusi termini e condizioni, richieste, obiettivi del livello di servizio e ore di servizio.

  https://support.ca.com/prodinfo/centappssupportofferings

- **Registrazione al Supporto tecnico** - Questo collegamento consente di accedere al modulo di registrazione in linea di CA Support, utile per l'attivazione del supporto per il prodotto.

  https://support.ca.com/prodinfo/supportregistration

- **Accesso al Supporto tecnico** - Questo collegamento consente di accedere alla pagina del supporto One-Stop di CA ARCserve Central Applications.

  https://support.ca.com/prodinfo/arccentapps

Modifiche apportate alla documentazione

Di seguito si elencano gli aggiornamenti apportati alla documentazione dall'ultima release CA ARCserve Central Host-Based VM Backup:

- Aggiornamento contenente commenti e suggerimenti degli utenti, correzioni e altre modifiche minori per migliorare le modalità di utilizzo e il funzionamento del prodotto o la documentazione stessa.
- Aggiornamento della sezione Creazione di criteri di backup (a pagina 76). Questo argomento include due nuove opzioni della scheda Impostazioni di backup/Avanzate: Riserva spazio sulla destinazione e Cataloghi. Inoltre, nella scheda Preferenze/Avvisi di posta elettronica sono state aggiunte due nuove funzionalità di unione dei processi ed è stata rimossa l'opzione Unione non riuscita.
- Aggiornamento della sezione Modifica o copia di criteri di backup (a pagina 80). Questo argomento include due nuove opzioni della scheda Impostazioni di backup/Avanzate: Riserva spazio sulla destinazione e Cataloghi.
- Aggiornamento della sezione Visualizzazione di registri CA ARCserve Central Host-Based VM Backup (a pagina 87). Questo argomento include due nuove opzioni nell'elenco a discesa Modulo: Aggiorna nodi multipli e Processo di unione CA ARCserve D2D.
- Aggiornamento della sezione Recupero di un intero computer virtuale (a pagina 104). Questa sezione è stata aggiornata per descrivere il nuovo aspetto della finestra di dialogo.
- Aggiornamento della sezione Errore di accesso negato durante l'aggiornamento dei nodi (a pagina 130). Questa sezione è stata aggiornata per includere due soluzioni per disabilitare il Controllo account utente (UAC).
- Aggiornamento della sezione Esecuzione di un ripristino bare metal (a pagina 161). Questa sezione è stata aggiornata per includere la nuova utilità di creazione del kit di avvio per il ripristino bare metal che consente di creare immagini WinPE ISO per l'esecuzione del ripristino bare metal. I file ISO non sono più forniti. Inoltre, questo argomento include il supporto del ripristino bare metal da un backup eseguito su un computer UEFI a un computer BIOS e da un computer BIOS a un computer UEFI.
- Aggiunta della sezione Creazione di un kit di avvio (a pagina 181). Questo argomento è stato aggiunto per includere le funzionalità della nuova utilità di creazione delle immagini WinPE ISO per l'esecuzione del ripristino bare metal.

  Nota: la sezione precedente Creazione di un kit di avvio è stata rimossa e sostituita dalla nuova sezione.
- Aggiornamento della sezione relativa al ripristino dell'applicazione Microsoft Exchange Server con nuove sezioni di scenario relative al Ripristino di un'applicazione Microsoft Exchange. Questa sezione include il supporto di Exchange 2013. Consultare la sezione Verifica delle considerazioni e dei prerequisiti di ripristino.

- Aggiunta della sezione CA ARCserve Central Host-Based VM Backup non riconosce i volumi sui dischi dinamici durante il recupero del computer virtuale su un server Hyper-V o un server ESX alternativo (a pagina 158). Questa sezione descrive la soluzione per il recupero dei volumi sui dischi dinamici.
- Aggiunta della sezione Esclusione di file dalla scansione antivirus (a pagina 201). Questo argomento descrive i file, le cartelle e i processi da escludere prima della scansione antivirus.
- Sono stati aggiornati i seguenti argomenti per fornire le credenziali integrate o dell'amministratore di dominio per accedere al sistema operativo guest del computer virtuale.
  - Attività preliminari all'installazione (a pagina 17)
  - Soluzioni per gli elementi di verifica preliminare (a pagina 61)
  - Errore di accesso negato durante l'aggiornamento dei nodi (a pagina 130)

Sommario

Capitolo 1: Introduzione a CA ARCserve Central Host-Based VM Backup

Questa sezione contiene i seguenti argomenti:

Introduzione

CA ARCserve Central Applications combina la protezione dei dati principali e le tecnologie di gestione con un ecosistema mirato di applicazioni che funzionano all'unisono al fine di facilitare la protezione, la copia, lo spostamento e la trasformazione dei dati on-premise e off-premise all'interno di ambienti globali.

Le applicazioni CA ARCserve Central Applications possono essere utilizzate, gestite e installate facilmente. Questa soluzione consente alle organizzazioni un controllo automatizzato delle informazioni al fine di prendere decisioni consapevoli sull'accesso, sulla disponibilità e sulla protezione dei dati in base al valore di business complessivo.

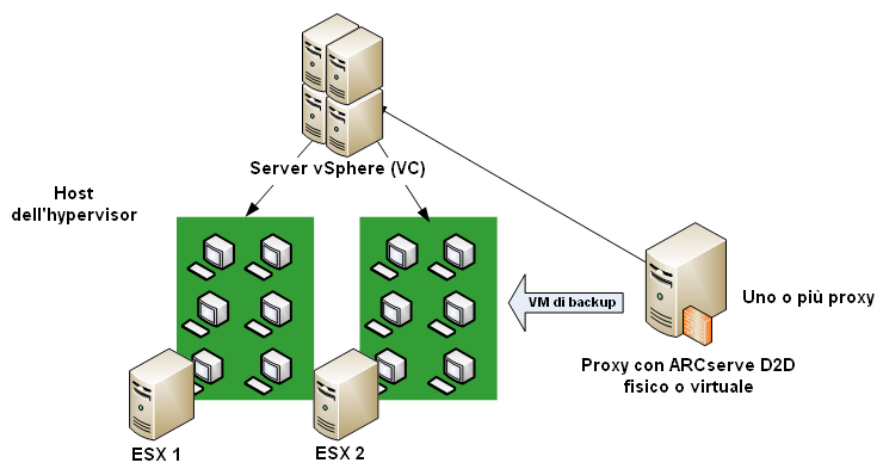
Informazioni su CA ARCserve Central Host-Based VM Backup

Una delle CA ARCserve Central Applications corrisponde all'applicazione CA ARCserve Central Host-Based VM Backup. Questa applicazione funziona con CA ARCserve D2D, una soluzione di backup a bassa densità, e consente di proteggere più computer virtuali senza dover installare il software o un agente su ciascun computer virtuale. Questa funzionalità riduce al minimo gli effetti negativi derivanti dall'esecuzione di più operazioni di backup sullo stesso server fisico e consente di eseguire backup a livello di file e di applicazione o ripristini bare metal dai backup del computer virtuale.

CA ARCserve Central Host-Based VM Backup è un'applicazione facilmente scalabile che consente di aggiungere computer virtuali in base alle proprie necessità senza dover acquistare licenze aggiuntive o installare software su ogni computer virtuale del proprio ambiente.

Modalità di funzionamento di CA ARCserve Central Host-Based VM Backup

CA ARCserve Central Host-Based VM Backup consente di proteggere i computer virtuali in esecuzione su un server ESX o vCenter in un singolo passaggio utilizzando un'istanza di CA ARCserve D2D installata su un proxy. Utilizzare il seguente elenco di controllo per iniziare:

1. Installare CA ARCserve D2D su un computer (fisico o virtuale) funzionante come proxy di backup dell'ambiente. Per le istruzioni di installazione, fare riferimento all'argomento sull'installazione di CA ARCserve D2D, all'interno della Guida utente di CA ARCserve D2D. Verificare che il proxy sia configurato correttamente.
2. Aggiungere i nodi da gestire. Specificare un server ESX per consentire all'applicazione di rilevare i computer virtuali in esecuzione su tale server e conformi ai requisiti.
3. Creare criteri di backup. Per ogni criterio, specificare il proxy di backup in cui è stato installato CA ARCserve D2D.
4. Assegnare criteri di backup a ciascun computer virtuale in modo da proteggere tutti i computer virtuali con l'istanza CA ARCserve D2D univoca in esecuzione sul proxy di backup.
5. Per gestire meglio l'ambiente del computer virtuale, è possibile creare gruppi di nodi. Ad esempio, è possibile raggruppare i nodi in base alla funzione commerciale o all'applicazione installata e quindi assegnare un criterio configurato per proteggere i nodi associati a una specifica funzione o che eseguono una determinata applicazione.

Bookshelf di CA ARCserve Central Applications

Gli argomenti contenuti nella Guida in linea di CA ARCserve Central Applications sono disponibili anche nella Guida per l'utente in formato PDF. La versione PDF più recente di questa guida e la Guida in linea sono accessibili dal Bookshelf di CA ARCserve Central Applications.

Nei file Note di rilascio di CA ARCserve Central Applications sono contenute informazioni relative ai requisiti di sistema, al supporto di sistemi operativi, al supporto per il recupero delle applicazioni e altre informazioni che può essere necessario conoscere prima di installare il prodotto. I file di Note di rilascio contengono inoltre un elenco di problemi noti di cui l'utente deve essere a conoscenza prima di utilizzare CA ARCserve Central Applications. La versione più recente delle note di rilascio è disponibile nel Bookshelf di CA ARCserve Central Applications.

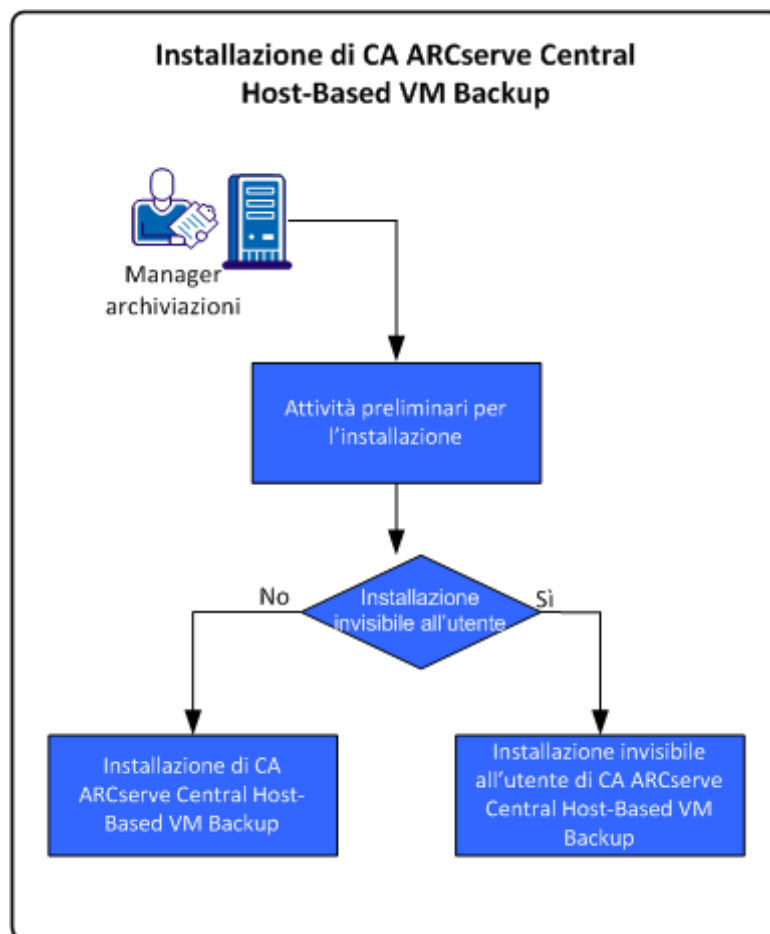
Capitolo 2: Installazione e configurazione di CA ARCserve Central Host-Based VM Backup

Questa sezione contiene i seguenti argomenti:

Installazione di CA ARCserve Central Host-Based VM Backup

Il presente scenario descrive la modalità di installazione di CA ARCserve Central Host-Based VM Backup per i manager dell'archiviazione mediante i seguenti metodi:

- Installazione standard - Il metodo in questione utilizza la procedura guidata per l'installazione dell'applicazione.
- Disinstallazione invisibile all'utente - Questo metodo consente di eseguire la disinstallazione automatica mediante la riga di comando di Windows.

Il diagramma seguente mostra la procedura di installazione dell'applicazione:

La tabella seguente elenca gli argomenti che descrivono le attività per l'installazione di CA ARCserve Central Host-Based VM Backup:

Attività	Argomento
Prima di installare l'applicazione, completare le attività di installazione preliminari e rivedere le considerazioni sull'installazione.	Attività preliminari all'installazione (a pagina 17)
Eseguire un'installazione standard mediante la procedura guidata di installazione.	Installazione di CA ARCserve Central Host-Based VM Backup (a pagina 19)
Eseguire la disinstallazione invisibile all'utente mediante la riga di comando di Windows.	sull'installazione di CA ARCserve Central Host-Based VM Backup in modalità invisibile all'utente (a pagina 21)

Per informazioni sull'aggiornamento di componenti del sistema operativo Windows dopo l'installazione dell'applicazione, consultare la sezione Procedura consigliata della Guida per l'utente di CA ARCserve Central Host-Based VM Backup.

Attività preliminari all'installazione

Prima di installare l'applicazione, completare le attività preliminari seguenti e verificare le considerazioni sull'installazione:

Operazioni preliminari

- Consultare il file delle Note di rilascio. Le Note di rilascio includono i requisiti di sistema, i sistemi operativi supportati e un elenco di problemi noti per questa versione dell'applicazione.
- Verificare che il sistema soddisfi i requisiti hardware e software minimi necessari per l'installazione dell'applicazione.
- Verificare che la funzionalità di traccia dei blocchi modificati sia abilitata sui computer virtuali protetti.

  Nota: per ulteriori informazioni sulla funzionalità di traccia dei blocchi modificati, consultare il seguente documento di informazioni di base sul sito Web di VMware:

  http://kb.vmware.com/kb/1020128
- Verificare che l'account Windows disponga dei privilegi di amministratore o equivalenti per l'installazione del software sui computer nei quali si desidera installare CA ARCserve Central Host-Based VM Backup.
- Verificare che l'account del server vCenter o ESX disponga di privilegi di amministratore Windows e VMware. È necessario assegnare l'account al ruolo di licenza globale sul sistema vCenter Server o ESX Server per consentire il completamento delle operazioni di VDDK.

- Verificare di disporre dei nomi utente e delle password dei computer su cui si sta procedendo all'installazione dell'applicazione di cui si è in possesso.
- Verificare che CA ARCserve D2D sia installato sul sistema proxy di backup designato per la protezione dei computer virtuali nell'ambiente di produzione.
- Se si desidera che il backup del computer virtuale disponga di capacità di ripristino granulare, verificare che vengano fornite le credenziali integrate o dell'amministratore di dominio degli utenti con privilegi amministrativi per consentire l'accesso al sistema operativo guest del computer virtuale.
- CA ARCserve Central Applications consente di installare CA ARCserve D2D e di eseguire l'aggiornamento della versione precedente all'ultima versione su nodi remoti mediante l'utilità di distribuzione. Per eseguire il backup dei dati sui nodi remoti utilizzando l'ultima versione di CA ARCserve D2D, è necessario disporre della versione più recente delle licenze di CA ARCserve D2D e applicare tali licenze sui nodi. Se le licenze non vengono applicate entro 31 giorni dalla data di installazione o di aggiornamento di CA ARCserve D2D sui nodi, il funzionamento di CA ARCserve D2D verrà interrotto.

Considerazioni sull'installazione

Prima di installare CA ARCserve Central Host-Based VM Backup, esaminare le seguenti considerazioni sull'installazione:

- Il pacchetto di installazione di CA ARCserve Central Applications installa un modulo denominato Server CA ARCserve Central Applications. Il server è un modulo comune a tutte le applicazioni. Il modulo contiene il servizio Web, i file binari e le configurazioni che consentono alle applicazioni di comunicare tra loro.

  Durante l'installazione dell'applicazione, il modulo server CA ARCserve Central Applications viene installato prima dei componenti del prodotto. Nel caso in cui fosse necessario applicare una patch all'applicazione, la patch aggiornerà il modulo prima di aggiornare i componenti del prodotto.
- Al completamento dell'installazione di CA ARCserve Central Host-Based VM Backup, scaricare e installare VMware VIX API versione 1.11 sul sistema proxy di backup e sul computer utilizzato per eseguire le verifiche preliminari. VMware VIX viene utilizzato per eseguire ripristini a livello di file e di applicazione dopo operazioni di backup.

  Nota: Per VIX API 1.11 è necessario che tutti i computer virtuali dispongano delle versioni più aggiornate degli strumenti VMware.
- CA ARCserve D2D esegue l'installazione di Virtual Disk Development Kit (VDDK) di VMware su tutti i computer su cui è installato CA ARCserve D2D. Non è necessario scaricare e installare VDDK sui sistemi proxy di backup.

  Se si desidera utilizzare una versione diversa di VDDK, scaricare e installare VDDK, quindi modificare il valore del registro di sistema di VDDKDirectory situato in HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA ARCSERVE D2D nella cartella di installazione del nuovo VDDK.

  La directory predefinita per VDDK è la seguente:

- **Sistema operativo X64**

  `c:\Program Files (x86)\VMware\VMware Virtual Disk Development Kit`

  Nota: decomprimere il file VDDK64.zip dalla directory di installazione nella cartella VDDK64.

  Ad esempio: c:\Program Files (x86)\VMware\VMware Virtual Disk Development Kit\VDDK64

- **Sistema operativo X86**

  `c:\Program Files\VMware\VMware Virtual Disk Development Kit`

- Alcune operazioni di ripristino richiedono l'installazione locale di CA ARCserve D2D. Per ulteriori informazioni, consultare l'argomento Considerazioni sul ripristino (a pagina 110). Le licenze di CA ARCserve D2D sono fornite con CA ARCserve Central Host-Based VM Backup. Per ottenere i file di installazione del prodotto, visitare il sito del Supporto tecnico di CA.
- Il mapping delle periferiche raw è supportato nella modalità di compatibilità virtuale ma non di compatibilità fisica.

Installazione di CA ARCserve Central Host-Based VM Backup

La procedura guidata di installazione consente all'utente di installare una o più applicazioni di CA ARCserve Central Applications.

Nota: prima di installare l'applicazione, consultare il file delle Note di rilascio e verificare che tutte le attività descritte nella sezioneAttività preliminari siano complete.

Per installare CA ARCserve Central Host-Based VM Backup

1. Scaricare il pacchetto di installazione di CA ARCserve Central Applications sul computer su cui si desidera installare l'applicazione, quindi fare doppio clic sul file di installazione.

   I contenuti del pacchetto di installazione verranno estratti sul computer e verrà visualizzata la finestra di dialogo Componenti richiesti.

2. Fare clic su Installa.

   Nota: la finestra di dialogo Componenti richiesti viene visualizzata solo se il programma di installazione non rileva che i componenti richiesti sono installati sul computer di destinazione.

   Al termine dell'installazione dei componenti richiesti, verrà visualizzata la finestra di dialogo Contratto di licenza.

3. Selezionare le opzioni necessarie, quindi fare clic su Avanti.

   Verrà visualizzata la finestra di dialogo Configurazione.

4. Sulla finestra di dialogo Configurazione, completare i seguenti campi:

   - **Componenti** - Specificare le applicazioni che si desidera installare.

     Nota: se l'applicazione viene installata mediante il pacchetto di installazione, è possibile installare più applicazioni simultaneamente.

   - **Posizione** - Accettare la posizione di installazione predefinita o fare clic su Sfogliare per specificare una posizione di installazione alternativa. La directory predefinita è la seguente:

     `C:\Programmi\CA\ARCserve Central Applications`

   - **Informazioni sul disco** - Verificare che il disco rigido disponga dello spazio sufficiente per l'installazione delle applicazioni.

   - **Nome dell'amministratore di Windows** - Specificare il nome utente dell'account di amministratore di Windows utilizzando la seguente sintassi:

     `Dominio\Nome utente`

   - **Password** - Specificare la password per l'account utente.

   - **Specificare il numero di porta** - Specificare il numero di porta da utilizzare per la comunicazione con l'interfaccia utente Web. Si consiglia di accettare il numero di porta predefinito. Il numero predefinito della porta è il seguente:

     `8015`

     Nota: per specificare un numero di porta alternativo, sarà necessario indicare un numero di porta compreso fra 1024 e 65535. Prima di indicare un numero di porta alternativo, verificare che il numero specificato sia libero e disponibile per l'uso. Il programma di installazione, infatti, non consente di installare l'applicazione se la porta selezionata non è disponibile per l'uso.

   - **Usa https per la comunicazione Web -** Specificare l'utilizzo della comunicazione HTTPS per la trasmissione dati. Per impostazione predefinita questa opzione è deselezionata.

     Nota: il protocollo HTTPS (protetto) fornisce un livello di protezione superiore rispetto alla comunicazione HTTP. Il protocollo di comunicazione HTTPS è consigliato se si trasmettono informazioni riservate sulla rete.

   - **Consenti al programma di installazione di registrare servizi/programmi di CA ARCserve Central Applications su Windows Firewall come eccezioni** - Verificare che la casella di controllo accanto a questa opzione sia selezionata. Le eccezioni firewall sono necessarie se si desidera configurare e gestire CA ARCserve Central Applications da computer remoti.

     Nota: per gli utenti locali, non è necessario registrare le eccezioni firewall.

   Fare clic su Avanti.

   Al completamento del processo di installazione, viene visualizzata la finestra Rapporto installazione.

5. La finestra di dialogo Rapporto installazione presenta un riepilogo di installazione. Per verificare la presenza di aggiornamenti per l'applicazione, fare clic su Verifica aggiornamenti e fare clic su Fine.

L'applicazione verrà installata.

sull'installazione di CA ARCserve Central Host-Based VM Backup in modalità invisibile all'utente

CA ARCserve Central Applications consente di installare CA ARCserve Central Host-Based VM Backup in modalità invisibile all'utente. Se si utilizza l'installazione invisibile all'utente, non sarà necessaria alcuna operazione da parte dell'utente. Di seguito è descritta la procedura per installare l'applicazione utilizzando la riga di comando di Windows.

Per installare CA ARCserve Central Host-Based VM Backup in modalità invisibile all'utente

1. Aprire la riga di comando di Windows nel computer in cui si desidera iniziare il processo di installazione invisibile all'utente.
2. Scaricare il pacchetto di installazione autoestraente di CA ARCserve Central Applications.

   Avviare il processo di installazione invisibile all'utente utilizzando la seguente sintassi della riga di comando:

   ```
   "CA ARCserve Central Applications Setup.exe" /s /v"/q -Path:<INSTALLDIR>
   -Port:<PORT> -U:<UserName> -P:<Password> -Products:<ProductList>"
   ```

   Uso:

   s

   Consente di avviare il pacchetto di file eseguibile in modalità invisibile all'utente.

   v

   Consente di specificare ulteriori opzioni della riga di comando.

   q

   Consente di installare l'applicazione in modalità invisibile all'utente.

-Percorso:<INSTALLDIR>

(Facoltativo) Consente di specificare il percorso di destinazione dell'installazione.

Esempio:

```
-Percorso:C:\Programmi\CA\ARCserve Central Applications
```

Nota: se il valore di INSTALLDIR contiene uno spazio, racchiudere il percorso tra virgolette e barre rovesciate. Inoltre, il percorso non può terminare con una barra rovesciata.

-Port:<PORTA>

(Facoltativo) Consente di specificare il numero di porta per la comunicazione.

Esempio:

```
-Port:8015
```

-U:<NomeUtente>

Consente di specificare il nome utente da utilizzare per installare ed eseguire l'applicazione.

Nota: il nome utente deve corrispondere a un account amministrativo o a un account con privilegi amministrativi.

-P:<Password>

Consente di specificare la password per il nome utente.

-Products:<Elenco prodotti>

(Facoltativo) Consente di specificare l'installazione in modalità invisibile all'utente di CA ARCserve Central Applications. Se non si specifica un valore per questo argomento, durante la procedura di installazione invisibile all'utente vengono installati tutti i componenti di CA ARCserve Central Applications.

CA ARCserve Central Host-Based VM Backup

VSPHEREX64

CA ARCserve Central Protection Manager

CMX64

CA ARCserve Central Reporting

REPORTINGX64

CA ARCserve Central Virtual Standby

VCMX64

Tutte le applicazioni CA ARCserve Central Applications

TUTTO

Nota: gli esempi riportati di seguito descrivono la sintassi per eseguire l'installazione di una o più applicazioni CA ARCserve Central Applications in modalità invisibile all'utente:

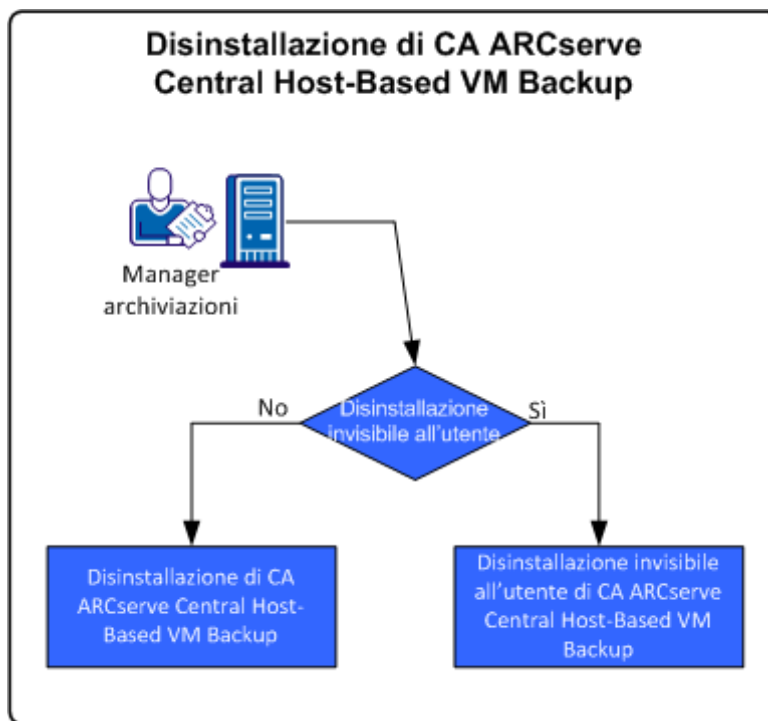
```
-Products:CMX64
-Products:CMX64,VCMX64
-Products:CMX64,VCMX64,REPORTINGX64
-Products:ALL
```

L'applicazione verrà installata in modalità invisibile all'utente.

Disinstallazione di CA ARCserve Central Host-Based VM Backup

Per eseguire la disinstallazione di CA ARCserve Central Host-Based VM Backup, utilizzare uno dei seguenti metodi:

- Disinstallazione standard - Questo metodo consente di disinstallare l'applicazione dal Pannello di controllo di Windows.
- Disinstallazione invisibile all'utente - Questo metodo consente di eseguire disinstallazioni non previste mediante la riga di comando di Windows.

Il diagramma seguente mostra la procedura di disinstallazione dell'applicazione:

Attività	Argomento
Disinstallazione standard mediante il Pannello di controllo di Windows.	Disinstallazione di CA ARCserve Central Host-Based VM Backup (a pagina 25)
Eseguire la disinstallazione invisibile all'utente mediante la riga di comando di Windows.	Disinstallazione di CA ARCserve Central Host-Based VM Backup in modalità invisibile all'utente. (a pagina 26)

Per informazioni sull'aggiornamento di componenti del sistema operativo Windows dopo la disinstallazione dell'applicazione, consultare la sezione Procedura consigliata della Guida per l'utente di CA ARCserve Central Host-Based VM Backup.

Disinstallazione di CA ARCserve Central Host-Based VM Backup

La disinstallazione delle applicazioni può essere effettuata anche da Programmi e funzionalità nel Pannello di controllo di Windows.

Per disinstallare CA ARCserve Central Host-Based VM Backup

1. Dal menu Start di Windows, fare clic su Pannello di controllo.

   Verrà visualizzato il Pannello di controllo di Windows.

2. Fare clic sull'elenco a discesa Visualizza quindi su Icone grandi o Icone piccole.

   Le icone del pannello di controllo di Windows verranno visualizzate in un layout griglia.

3. Fare clic su Programmi e funzionalità.

   Verrà visualizzata la finestra Disinstalla o modifica programma.

4. Individuare e fare clic sull'applicazione che si desidera disinstallare.

   Fare clic con il pulsante destro del mouse sull'applicazione, quindi fare clic su Disinstalla dal menu di scelta rapida.

   Seguire le istruzioni visualizzate sullo schermo per completare la disinstallazione.

L'applicazione verrà disinstallata.

Disinstallazione di CA ARCserve Central Host-Based VM Backup in modalità invisibile all'utente.

CA ARCserve Central Applications consente di disinstallare CA ARCserve Central Host-Based VM Backup in modalità invisibile all'utente. Se si utilizza l'installazione invisibile all'utente, non sarà necessario alcun intervento da parte dell'utente. Di seguito è descritta la procedura per disinstallare l'applicazione utilizzando la riga di comando di Windows.

Per disinstallare CA ARCserve Central Host-Based VM Backup in modalità invisibile all'utente

1. Accedere al computer da cui si desidera disinstallare l'applicazione.

   Nota: è necessario accedere con un account amministrativo o un account con privilegi amministrativi.

2. Aprire la riga di comando di Windows ed eseguire il seguente comando per avviare il processo di disinstallazione invisibile all'utente:

   ```
   <INSTALLDIR>%\Setup\uninstall.exe /q /p <ProductCode>
   ```

   Oppure

   ```
   <INSTALLDIR>%\Setup\uninstall.exe /q /p <ALL>
   ```

   Esempio: la sintassi seguente consente di disinstallare CA ARCserve Central Host-Based VM Backup in modalità invisibile all'utente.

   ```
   "%Programmi%\CA\ARCserve Central Applications\Setup\uninstall.exe" /q /p
   {CAED49D3-0D3C-4C59-9D99-33AFAF0C7126}
   ```

Uso:

<INSTALLDIR>

Consente di specificare la directory in cui è installata l'applicazione.

Nota: eseguire la sintassi corrispondente all'architettura del sistema operativo del computer.

<CodiceProdotto>

Consente di specificare l'applicazione da disinstallare in modalità invisibile all'utente.

Nota: la procedura di disinstallazione invisibile all'utente consente di installare una o più applicazioni di CA ARCserve Central Applications. Utilizzare i seguenti codici di prodotto per disinstallare CA ARCserve Central Applications in modalità invisibile all'utente:

CA ARCserve Central Host-Based VM Backup

{CAED49D3-0D3C-4C59-9D99-33AFAF0C7126}

CA ARCserve Central Protection Manager

{CAED05FE-D895-4FD5-B964-001928BD2D62}

CA ARCserve Central Reporting

{CAED8DA9-D9A8-4F63-8689-B34DEEEEC542}

CA ARCserve Central Virtual Standby

{CAED4835-964B-484B-A395-E2DF12E6F73D}

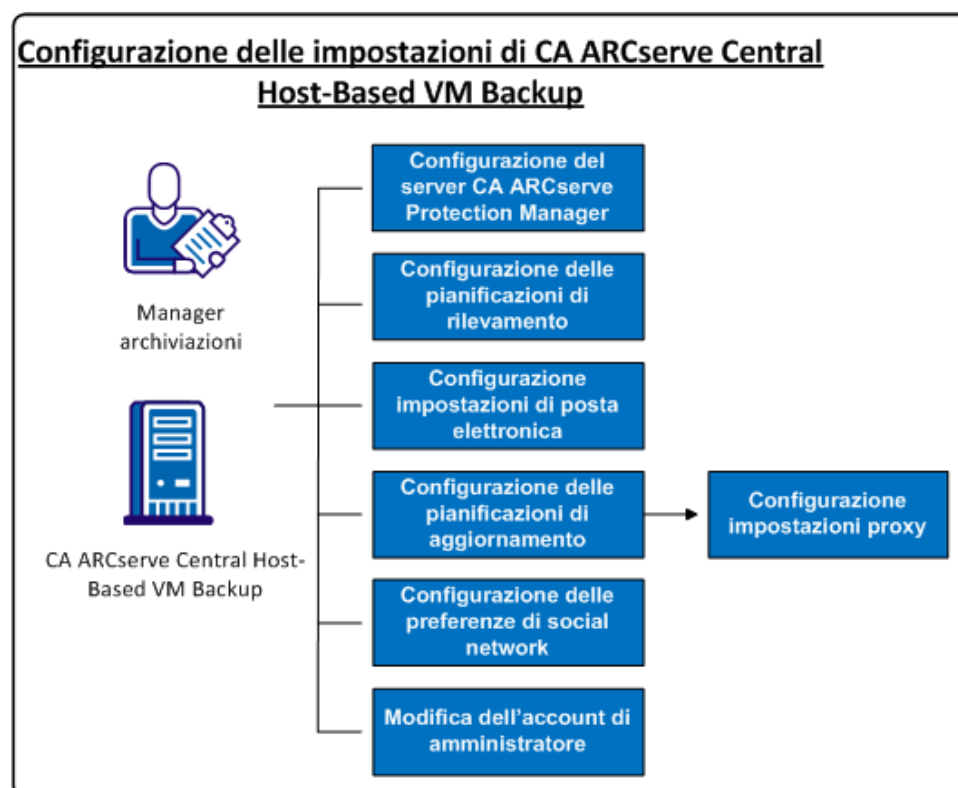
L'applicazione verrà disinstallata in modalità invisibile all'utente.

Configurazione di CA ARCserve Central Host-Based VM Backup per la protezione dei nodi CA ARCserve D2D

L'applicazione consente di specificare le impostazioni di configurazione per i messaggi di posta elettronica di avviso e le pianificazioni, nonché descrive la modalità di aggiornamento dell'installazione di CA ARCserve Central Host-Based VM Backup.

Prima di specificare le impostazioni della configurazione, è necessario installare CA ARCserve D2D sul server che esegue i processi di backup. Questo server peer o proxy può essere composto da uno o più computer, a seconda delle proprie esigenze. Per istruzioni, consultare l'argomento relativo all'installazione di CA ARCserve D2D dalla Guida per l'utente di CA ARCserve D2D.

CA ARCserve Central Host-Based VM Backup può essere installato sullo stesso computer o su un computer differente. La procedura di installazione si basa su una procedura guidata che consente un'installazione semplice. Per ulteriori informazioni, consultare la sezione Installazione di CA ARCserve Central Host-Based VM Backup.

L'illustrazione seguente descrive i tipi di configurazione che è possibile impostare per l'applicazione:

Il presente scenario descrive i seguenti argomenti:

- Configurazione del server CA ARCserve Central Protection Manager (a pagina 29)

Configurazione del server CA ARCserve Central Protection Manager

La configurazione del server CA ARCserve Central Protection Manager consente di modificare le impostazioni correnti di CA ARCserve Central Host-Based VM Backup a quelle del server CA ARCserve Central Protection Manager. Una volta configurate le impostazioni, è possibile visualizzare le informazioni dei messaggi di avviso di posta elettronica sui nodi CA ARCserve Central Host-Based VM Backup rilevati da CA ARCserve Central Reporting.

Procedere come descritto di seguito:

1. Accedere al server CA ARCserve Central Host-Based VM Backup e fare clic su Configurazione nella barra di navigazione.

   Verrà visualizzata la schermata Configurazione.

2. Dal pannello Configurazione, fare clic su Configurazione CA ARCserve Central Protection Manager.

3. Completare i seguenti campi:

   - **Server CA ARCserve Central Protection Manager**

     Nota: dopo aver installato CA ARCserve Central Protection Manager e CA ARCserve Central Host-Based VM Backup, i valori dei campi seguenti vengono sostituiti con i valori predefiniti del server CA ARCserve Central Protection Manager locale. Se CA ARCserve Central Protection Manager non è installato, i campi rimarranno vuoti e sarà necessario eseguire la configurazione manuale. CA ARCserve Central Reporting consente di visualizzare le informazioni relative ai nodi rilevati.

- **Nome computer** - Il nome host del computer in cui è installato CA ARCserve Central Protection Manager.
    - **Nome utente** - Il nome utente richiesto per l'accesso al computer su cui è installato CA ARCserve Central Protection Manager.
    - **Password** - La password per l'utente.
    - **Porta** - Il numero della porta da utilizzare per comunicare con il servizio Web di CA ARCserve Central Protection Manager.
    - **HTTPS** - Questa opzione è selezionata o deselezionata in base alla connessione configurata sul server CA ARCserve Central Protection Manager.
- **Rileva automaticamente la porta e il protocollo** - Consente di acquisire la porta e il protocollo CA ARCserve Central Protection Manager del database di Protection Manager e compila i campi soprastanti.

  Nota: questa opzione è disponibile solo in caso di autorizzazione di accesso al Registro di sistema remoto del server CA ARCserve Central Protection Manager.

  Per verificare la validità del Registro di sistema remoto, eseguire le seguenti operazioni:

    1. Accedere al server CA ARCserve Central Protection Manager su cui è installato CA ARCserve Central Protection Manager.
    2. Accedere a services.msc e verificare che il servizio Registro di sistema remoto sia stato avviato.
    3. Impostare l'opzione su Automatico.
- **Test** - Consente di verificare se le informazioni di accesso a CA ARCserve Central Protection Manager sono corrette.

4. Fare clic su Salva.

Configurazione delle pianificazioni di rilevamento

La pianificazione di rilevamento automatico dei nodi può essere impostata su base ricorrente o ad un'ora specificata. Per impostazione predefinita, la configurazione di rilevamento automatico è disabilitata. Per abilitare la configurazione, fare clic sull'opzione Abilita per specificare il tipo di ricorrenza desiderato e l'ora pianificata per l'avvio del rilevamento automatico. È possibile specificare i seguenti parametri di configurazione della pianificazione di rilevamento:

- **Ogni numero di giorni** - Ripete il metodo in base al numero di giorni specificato. (Impostazione predefinita).
- **Ogni giorno della settimana selezionato** - Ripete il metodo nei giorni della settimana specificati. Lunedì, martedì, mercoledì, giovedì e venerdì sono i giorni predefiniti della settimana.
- **Ogni giorno del mese selezionato** - Ripete il metodo nel giorno del mese specificato. Il valore predefinito per il giorno del mese è 1.

Viene visualizzato l'elenco Host vCenter/ESX indicante la data di impostazione di una pianificazione per il rilevamento dei nodi.

Configurazione delle impostazioni dei messaggi di posta elettronica e di avviso

Le impostazioni di posta elettronica e di avviso possono essere configurate per l'invio automatico degli avvisi nel caso in cui si verifichino le condizioni specificate.

Procedere come descritto di seguito:

1. Accedere all'applicazione.

   Dalla barra di navigazione della pagina principale, fare clic su Configurazione per aprire la schermata corrispondente.

2. Dal riquadro Configurazione, fare clic su Configurazione posta elettronica e avvisi per aprire l'opzione Configurazione posta elettronica e avvisi.

3. Completare i seguenti campi:
   - **Servizio** - Specificare il tipo di servizio di posta elettronica dall'elenco a discesa. (Google Mail, Yahoo Mail, Live Mail o Altri).
   - **Server di posta** - Specificare il nome host del server SMTP utilizzato da CA ARCserve Central Applications per l'invio di messaggi di posta elettronica.
   - **Richiede l'autenticazione** - Selezionare questa opzione se il server di posta specificato richiede l'autenticazione. Il Nome account e la Password sono obbligatori.
   - **Oggetto** - Specificare un oggetto di posta elettronica predefinito.
   - **Da** - Specificare l'indirizzo di posta elettronica di invio del messaggio.
   - **Destinatari** - Specificare uno o più indirizzi di posta elettronica, separati da un punto e virgola (;), per l'invio di messaggi di posta elettronica.
   - **Usa SSL** - Selezionare questa opzione se il server di posta specificato richiede la connessione protetta (SSL).
   - **Invia STARTTLS** - Selezionare questa opzione se il server di posta specificato richiede il comando STARTTLS.
   - **Usa formato HTML** - Consente di inviare messaggi di posta elettronica in formato HTML. (selezionato per impostazione predefinita)
   - **Abilita impostazioni proxy** - Selezionare questa opzione se è presente un server proxy, quindi specificare le impostazioni corrispondenti.
4. Fare clic su Messaggio di posta elettronica di verifica per verificare che le impostazioni di configurazione siano corrette.
5. (Facoltativo) Dalla sezione Invia avvisi tramite posta elettronica, fare clic su Nodi rilevati per consentire all'applicazione di inviare messaggi di posta elettronica di avviso al rilevamento di nuovi nodi.
6. Fare clic su Salva.

   Nota: è possibile fare clic su Reimposta per ripristinare i valori salvati precedentemente, oppure fare clic su Elimina per eliminare le impostazioni salvate. L'eliminazione delle impostazioni di posta elettronica e di avviso impediscono la ricezione dei messaggi di posta elettronica di avviso.

La configurazione del server di posta verrà applicata.

Configurazione delle pianificazioni di aggiornamento

È possibile impostare una pianificazione per il download automatico degli aggiornamenti di prodotto da un server CA oppure da un server di gestione temporanea software locale.

Procedere come descritto di seguito:

1. Accedere all'applicazione.
2. Fare clic su Configurazione sulla barra di navigazione per aprire la schermata Configurazione.
3. Dal pannello di configurazione, fare clic su Configurazione aggiornamento.

   Verranno visualizzate le opzioni di configurazione degli aggiornamenti.
4. Selezionare un server di download.
   - **CA Server** - Fare clic su Impostazioni proxy per visualizzare le opzioni seguenti:
     - **Utilizza le impostazioni proxy del browser** - Consente di utilizzare le credenziali immesse per il proxy del browser.

       Nota: l'opzione Utilizza le impostazioni proxy del browser influisce sul funzionamento di Internet Explorer e Chrome.
     - **Configura impostazioni proxy** - Specificare l'indirizzo IP o il nome host del server proxy e il numero di porta. Se il server specificato richiede l'autenticazione, selezionare l'opzione Il server proxy richiede l'autenticazione e immettere le credenziali.

       Fare clic su OK per tornare alla configurazione aggiornamenti.
   - **Server di gestione temporanea** - Se si sceglie questa opzione, fare clic su Aggiungi server per aggiungere un server di gestione temporanea all'elenco. Immettere il nome host e il numero di porta del server, quindi fare clic su OK.

     Se si specificano più server di gestione temporanea, l'applicazione tenterà di utilizzare il primo server contenuto nell'elenco. Se la connection viene eseguita correttamente, i server restanti non verranno utilizzati per la gestione temporanea.
5. (Facoltativo) Per verificare la connessione del server, fare clic su Verifica connessione e attendere il completamento della verifica.
6. (Facoltativo) Fare clic Verifica aggiornamenti automaticamente e specificare il giorno e l'ora desiderati. La pianificazione può essere effettuata su base giornaliera o settimanale.

Fare clic su Salva per applicare la configurazione di aggiornamento.

Configura impostazioni proxy

CA ARCserve Central Applications consente di specificare un server proxy per la comunicazione con il supporto tecnico di CA per verificare la disponibilità di aggiornamenti e scaricarli. Per attivare questa funzionalità, specificare il server proxy che si desidera impostare per la comunicazione del server CA ARCserve Central Applications.

Procedere come descritto di seguito:

1. Accedere all'applicazione e fare clic su Configurazione sulla barra di spostamento.

   Verranno visualizzate le opzioni di configurazione.

2. Fare clic su Configurazione aggiornamento.

   Verrà visualizzata la finestra di dialogo Configurazione aggiornamento.

3. Fare clic su Impostazioni proxy.

   Verrà visualizzata la finestra di dialogo Impostazioni proxy.

4. Selezionare una delle seguenti opzioni:

   - **Utilizza le impostazioni proxy del browser** - Consente all'applicazione di rilevare e utilizzare le stesse impostazioni proxy applicate al browser per connettersi al server di CA Technologies per aggiornare le informazioni.

     Nota: questo comportamento è valido solo per i browser Internet Explorer e Chrome.

   - **Configura impostazioni proxy** - Consente di definire un server alternativo che l'applicazione utilizzerà per comunicare con il Supporto tecnico di CA per verificare la disponibilità di aggiornamenti. Il server alternativo (proxy) garantisce protezione e migliora le prestazioni e il controllo amministrativo.

     Completare i seguenti campi:

     - **Server proxy** - Specificare il nome host o l'indirizzo IP del server proxy.
     - **Porta** - Specificare il numero di porta che il server proxy utilizzerà per comunicare con il sito Web del Supporto tecnico di CA.
     - **(Facoltativo) Il server proxy richiede l'autenticazione -** Se le credenziali di accesso per il server proxy non sono uguali a quelle per il server CA ARCserve Central Applications, selezionare la casella di controllo Il server proxy richiede l'autenticazione e specificare il nome utente e la password per l'accesso al server proxy.

       Nota: per specificare il nome utente utilizzare il formato <nome dominio>/<nome utente>.

   Fare clic su OK.

Le impostazioni proxy sono configurate.

Nota: per garantire la distribuzione dei criteri sui nodi e la protezione dei nodi di CA ARCserve D2D, verificare che il server CA ARCserve Central Host-Based VM Backup e il server proxy siano in grado di comunicare l'uno con l'altro mediante i loro nomi host. Procedere come segue:

1. Sul server CA ARCserve Central Host-Based VM Backup, eseguire il ping del server proxy utilizzando i nomi host del server.
2. Sul server proxy, eseguire il ping verso il server CA ARCserve Central Host-Based VM Backup utilizzando il nome host del server.

Configurazione delle preferenze di Social network

CA ARCserve Central Applications consente di gestire gli strumenti di Social network che possono agevolare la gestione delle singole applicazioni. È possibile generare newsfeed, specificare collegamenti a siti Web di social network popolari e selezionare siti Web video.

Procedere come descritto di seguito:

1. Accedere all'applicazione.

   Dalla barra di navigazione della pagina principale, fare clic su Configurazione per aprire la schermata corrispondente.

2. Dal riquadro Configurazione, fare clic su Configurazione delle preferenze per aprire le opzioni Preferenze.

3. Specificare le opzioni desiderate:

   - **Newsfeed** - L'applicazione visualizza i feed RSS relativi alle notizie più recenti di CA ARCserve Central Applications e CA ARCserve D2D e le informazioni sui prodotti dal Centro di consultazione esperti. I feed verranno visualizzati nella pagina principale.
   - **Social network** - L'applicazione visualizza nella pagina principale le icone di accesso a Twitter e Facebook per i siti Web di social network relativi a CA ARCserve Central Applications e CA ARCserve D2D.
   - **Video** - Consente di selezionare il tipo di video per la visualizzazione dei prodotti CA ARCserve Central Applications e CA ARCserve D2D (Impostazione predefinita: Video di YouTube).

   Fare clic su Salva.

   Le opzioni di Social network verranno applicate

4. Dalla barra di navigazione fare clic su pagina iniziale.

   Verrà visualizzata la pagina iniziale.

5. Aggiornare il browser.

   Le opzioni di Social network verranno applicate.

Modificare l'account di amministratore

CA ARCserve Central Applications consente di modificare il nome utente e/o la password per l'account dell'amministratore dopo l'installazione dell'applicazione. L'account di amministratore viene utilizzato solo per il nome utente predefinito visualizzato sulla schermata di accesso.

Nota: il nome utente specificato deve essere un account amministrativo di Windows o un account che dispone di privilegi di amministratore di Windows.

Procedere come descritto di seguito:

1. Accedere all'applicazione e fare clic su Configurazione sulla barra di spostamento.

   Vengono visualizzate le opzioni di configurazione.

2. Fare clic su Account di amministratore

3. Vengono visualizzate le impostazioni dell'account di amministratore.

4. Aggiornare i seguenti campi:

   - Nome utente
   - Password

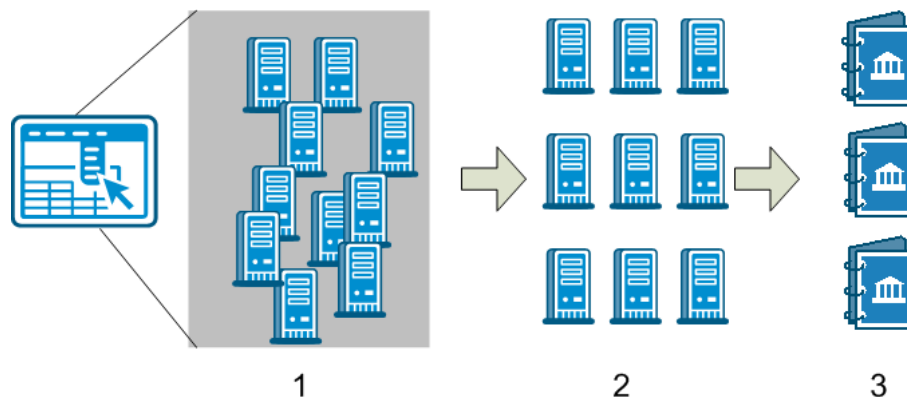
   Fare clic su Salva.

L'account di amministratore viene modificato.

Capitolo 3: Utilizzo di CA ARCserve Central Host-Based VM Backup

Questa sezione contiene i seguenti argomenti:

Impostazione dell'ambiente di produzione

La protezione dell'ambiente del computer virtuale richiede alcune semplici azioni:

1. Aggiunta di nodi a CA ARCserve Central Host-Based VM Backup. È possibile importare tutti i computer virtuali che risiedono su un server ESX o vCenter.
2. Raggruppare i nodi per facilitarne la gestione, Ad esempio, è possibile raggrupparli per funzione di business o per applicazioni installate.
3. Infine, creare criteri di backup e assegnare ogni criterio a un gruppo. Tutti i nodi verranno sottoposti a backup in base al criterio impostato.

Modalità di utilizzo della pagina principale di CA ARCserve Central Host-Based VM Backup

L'avvio di CA ARCserve Central Host-Based VM Backup comporta la visualizzazione della pagina principale nel browser Web. Dalla pagina principale è possibile eseguire le seguenti operazioni:

- **Navigazione nella parte sinistra**:
  - **Nodo** - La schermata Nodo consente di visualizzare l'ambiente del computer virtuale in base ai gruppi di nodi, alle applicazioni installate e al criterio vSphere assegnato.
  - **Criteri** - La schermata Criteri vSphere consente di creare, modificare e assegnare criteri di backup a tutti i nodi presenti nell'ambiente.
  - **Configurazione** - La schermata Configurazione consente di specificare gli avvisi di posta elettronica e la pianificazione di aggiornamento automatico per l'applicazione.
  - **Visualizza registri** - La schermata Visualizza registri consente di individuare problemi specifici come informazioni, errori e avvisi.
  - **Aggiungi nuova scheda** - Consente di aggiungere manualmente il nome e l'URL di qualunque sito Web che si desidera monitorare.
  - **Supporto tecnico di CA** - Consente di accedere a vari siti di supporto e social network, inclusi Facebook e Twitter.

Accesso ai nodi CA ARCserve D2D

L'accesso ai nodi di CA ARCserve D2D può essere eseguito dalla pagina principale del backup dei computer virtuali basato sull'host.

Per accedere ai nodi CA ARCserve D2D

1. Aprire l'applicazione e fare clic su Nodi sulla barra di navigazione.

   Verrà visualizzata la schermata Nodo.

2. Dall'elenco Gruppi, fare clic su Tutti i nodi oppure sul gruppo contenente il nodo CA ARCserve D2D a cui si desidera accedere.

   Nell'elenco dei nodi verranno visualizzati tutti i nodi associati al gruppo specificato.

3. Individuare e fare clic sul nodo a cui si desidera accedere, quindi su Accesso a D2D dal menu di scelta rapida.

   Viene aperta la versione CA ARCserve Central Host-Based VM Backup di CA ARCserve D2D.

   Nota: se non viene aperta una nuova finestra, verificare che le opzioni del browser non blocchino la visualizzazione di tutti i popup o di quelli del sito Web corrente.

L'utente è connesso al nodo CA ARCserve D2D.

Nota: è possibile che durante il primo accesso al nodo CA ARCserve D2D venga visualizzata una pagina HTML contenente un messaggio di avviso. Questo comportamento si verifica con l'utilizzo di Internet Explorer. Per risolvere il problema, chiudere Internet Explorer e ripetere il passaggio 3. Sarà quindi possibile accedere al nodo CA ARCserve D2D correttamente.

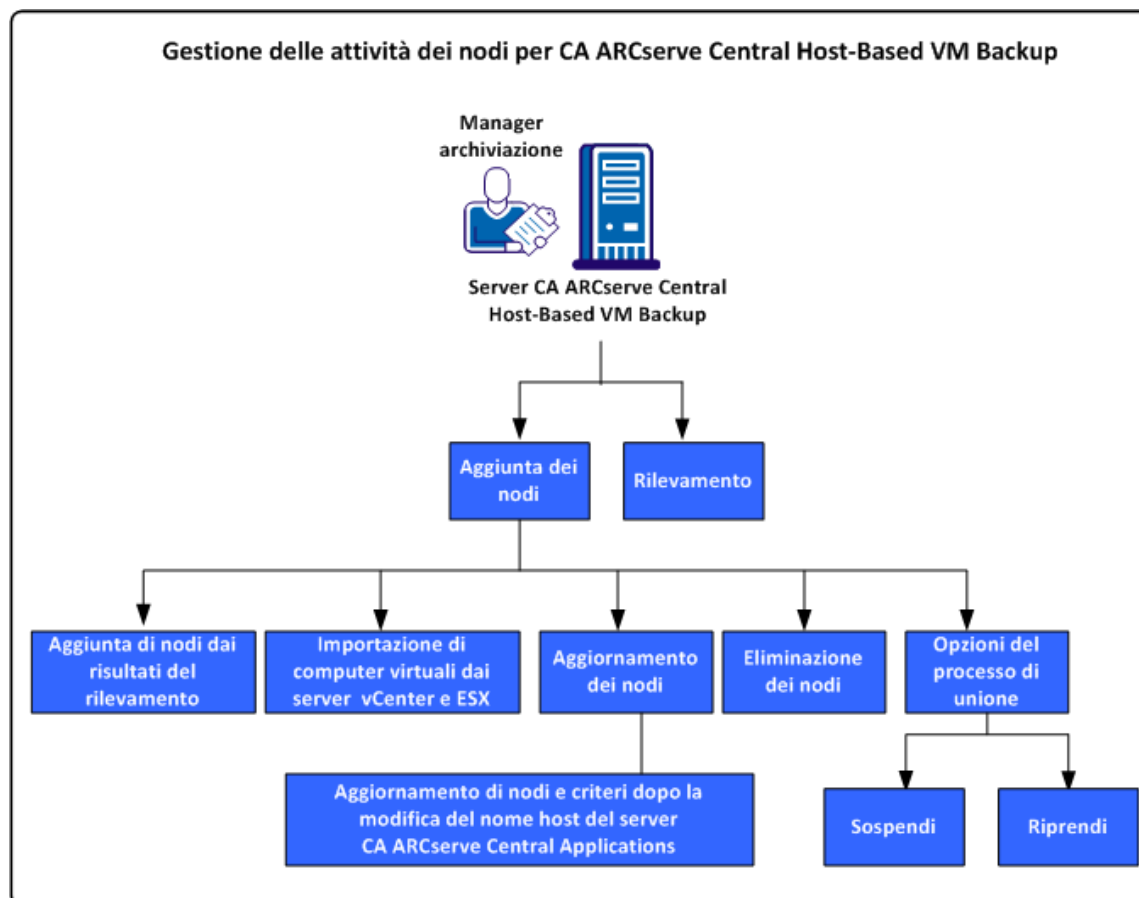
Modalità di gestione delle attività dei nodi per CA ARCserve Central Host-Based VM Backup

Questo scenario descrive la procedura eseguita dai manager dell'archiviazione per la gestione dei nodi. Ad esempio, l'aggiunta o il rilevamento di nodi, l'assegnazione di nodi al gruppo nodi e l'aggiornamento o l'eliminazione dei nodi della schermata Nodo.

La seguente tabella descrive gli elementi visualizzati nella schermata Nodo:

Nome colonna	Descrizione
Nome nodo	Visualizza il nome del nodo **Nota**: è possibile che alcuni nodi elencati non siano abilitati per la selezione. Ciò è dovuto al fatto che il nodo non può essere rilevato dal server. Ad esempio, è possibile eliminare il nodo del server.
Criterio	Visualizza il nome del criterio e lo stato di distribuzione del criterio.
Nome del computer virtuale	Visualizza il nome del computer virtuale.
vCenter/ESX	Visualizza i dettagli del server che consentono di individuare i computer virtuali.
Processo (a pagina 72)	Visualizza lo stato del processo di backup e contiene un collegamento alla sezione Monitoraggio dello stato di backup (a pagina 73) per ulteriori dettagli.

Nome colonna	Descrizione
Stato	Visualizza lo stato del nodo ■ = Errore/Operazione non riuscita ■ = Avviso ■ = Operazione eseguita correttamente Se si posiziona il mouse sull'icona, verrà visualizzata la tabella pop-up Riepilogo stato del nodo contenente i risultati relativi alle seguenti categorie: ■ Ultimo Backup - Visualizza il tipo, la data, l'ora e lo stato del backup. ■ Punti di ripristino - Visualizza il numero di punti di ripristino per il server monitorato. ■ Capacità di destinazione - Visualizza la quantità di spazio libero disponibile nella destinazione di backup.
Risultati dell'ultimo backup	Visualizza lo stato dell'ultimo processo di backup.
Ora ultimo backup	Visualizza la data e l'ora di esecuzione dell'ultimo processo di backup.
Stato verifica preliminare	Visualizza lo stato della verifica preliminare per i processi di backup: ■ = Errore/Operazione non riuscita ■ = Avviso ■ = Operazione eseguita correttamente L'icona indica se un processo di backup può essere o non essere eseguito per il nodo specificato. Se si posiziona il mouse sull'icona, verrà visualizzata la tabella pop-up Verifica contenente i risultati relativi alle seguenti categorie: ■ Funzionalità di traccia dei blocchi modificati - Visualizza i risultati corrispondenti per il backup. ■ Strumenti VMware - Indica se lo strumento VMware è stato installato. ■ Disco - Visualizza lo stato del disco. ■ Stato alimentazione - Indica se il computer virtuale è attivato. ■ Credenziali - Visualizza lo stato delle credenziali utente. ■ Applicazioni - Visualizza lo stato di installazione dell'applicazione sul nodo. Per ulteriori informazioni, consultare l'argomento Esecuzione di verifiche preliminare per i processi di backup (a pagina 60).
Applicazioni	Visualizza l'applicazione a cui è associato il nodo.
Sistema operativo	Visualizza il sistema operativo a cui è associato il nodo.
Descrizione	Visualizza una descrizione del nodo.

Il diagramma seguente illustra le attività che è possibile eseguire sui nodi.

Questo scenario descrive le opzioni che è possibile utilizzare durante l'aggiunta o l'aggiornamento di nodi:

- Rilevamento (a pagina 45)
- Aggiunta di nodi (a pagina 46)
  - Aggiunta automatica di nodi dai risultati di rilevamento automatico (a pagina 47)
  - Importazione di computer virtuali da server vCenter/ESX (a pagina 48)
- Aggiornamento dei nodi (a pagina 49)
  - Aggiornamento di nodi e criteri dopo la modifica del nome host del server CA ARCserve Central Applications (a pagina 50)
- Eliminazione dei nodi (a pagina 51)
- Opzioni del processo di unione (a pagina 51)
  - Interruzione di un processo di unione su un nodo (a pagina 51)
  - Ripresa di un processo di unione su un nodo (a pagina 52)

Rilevamento dei nodi da CA ARCserve Central Host-Based VM Backup

CA ARCserve Central Host-Based VM Backup consente il rilevamento di nodi in maniera automatica mediante l'aggiunta di sistemi server vCenter e ESX al proprio ambiente. In questo modo l'applicazione è in grado di rilevare i computer virtuali ospitati automaticamente.

Importante. Il processo di rilevamento dei nodi richiede all'utente di specificare il nome host o l'indirizzo IP del sistema server vCenter o ESX. Grazie a queste informazioni, il processo di rilevamento è in grado di individuare i computer virtuali collegati al sistema server vCenter o ESX. Se il nome host o l'indirizzo IP di un sistema server vCenter o ESX viene modificato, ripetere le operazioni descritte in questa sezione e distribuire nuovamente il criterio di backup per creare un nuovo set di backup contenente il nome host o l'indirizzo IP aggiornato.

Procedere come descritto di seguito:

1. Accedere all'applicazione e fare clic su Nodo della barra Navigazione per aprire la schermata Nodo.
2. Fare clic su Rileva della barra degli strumenti per aprire la finestra di dialogo Rileva nodi mediante server vCenter/ESX.
3. Completare i seguenti campi della finestra di dialogo Rileva nodi mediante server vCenter/ESX:
   - Host vCenter/ESX
   - Nome utente

     Nota: l'account specificato deve essere un account amministrativo o un account con privilegi amministrativi nel sistema del server ESX o vCenter.
   - Password
   - Porta

   Fare clic su Aggiungi.

   Nota: ripetere l'operazione per aggiungere ulteriori sistemi server vCenter/ESX.
4. Fare clic su Rileva per avviare il processo di rilevamento.

   Verrà visualizzato il Monitor di rilevamento, contenente l'avanzamento del rilevamento.
5. Al termine del processo di rilevamento, verrà visualizzato un messaggio di conferma: Continuare ad aggiungere nodi dai risultati di rilevamento?

   Fare clic su Sì e verrà visualizzata la schermata Aggiungere nodi dai risultati di rilevamento, oppure fare clic su No se si desidera aggiungere ulteriori hypervisor.

   Nota: per individuare i nodi automaticamente e aggiungerli all'elenco Nome nodo, consultare la sezione Configurazione delle pianificazioni di rilevamento per ulteriori dettagli.

6. Dall'elenco Nodi rilevati, selezionare i nodi che si desidera aggiungere, quindi fare clic sulla freccia destra. I nodi vengono aggiunti all'elenco dei nodi da proteggere.
7. Fare clic su Avanti per aprire la schermata Credenziali nodo.
8. Fornire un nome utente e una password per ogni nodo da aggiungere o specificare le credenziali globale appropriate.

   Fare clic su Fine.

   I nodi selezionati vengono aggiunti all'elenco dei nomi dei nodi nella schermata Nodo per il Gruppo nodi selezionato.
9. (Facoltativo) Fare clic su Aggiorna. Il server aggiunto è ora indicato nell'elenco Gruppi della schermata Nodo.
10. (Facoltativo) Fare clic su Rileva e ripetere le operazioni precedenti fino all'aggiunta di tutti i server.

Aggiunta di nodi

È possibile utilizzare la schermata Nodo per aggiungere nodi e assegnarli ai gruppi che si desidera gestire nell'applicazione. L'applicazione consente di aggiungere solo i computer virtuali con:

- Sistema operativo guest Windows
- Versione hardware VMware 7 o successiva.

È possibile aggiungere nodi mediante i processi seguenti:

- Aggiungi nodi dai risultati di rilevamento (a pagina 47) - Il rilevamento consente di immettere i dettagli del server ESX e vCenter, rilevare i computer virtuali in esecuzione su ogni server e aggiungere, manualmente o automaticamente, i nodi rilevati all'applicazione per la loro gestione e protezione.

  I server aggiunti all'elenco di rilevamento vengono analizzati in base alla pianificazione specificata nella schermata di configurazione fino a quando non saranno rimossi. Non sarà necessario immettere nuovamente i dettagli del server. L'elenco di rilevamento visualizza soltanto i nuovi computer virtuali aggiunti a un server dall'ultima analisi. Non mostra i computer virtuali già gestiti nell'applicazione. Inoltre, è possibile eseguire il rilevamento senza dover attendere l'analisi pianificata successiva.
- Importa computer virtuali da vCenter/ESX (a pagina 48)

  Questa opzione è un processo manuale. Il processo richiede la specificazione dei dettagli del server ESX o vCenter ogni volta che viene avviato. È possibile aggiungere server all'elenco di rilevamento se non si desidera immettere nuovamente i dettagli del server. Questa opzione elenca tutti i computer virtuali rilevati sul server specificato, inclusi quelli già gestiti nell'applicazione.

Aggiunta di nodi dai risultati del rilevamento

Questa opzione consente di selezionare i nodi rilevati automaticamente in base alle impostazioni specificate nel pannello Configurazione rilevamento.

Procedere come descritto di seguito:

1. Accedere all'applicazione.

   Fare clic su Nodi nella barra di navigazione per aprire la schermata Nodi.

2. Dalla categoria Nodo, fare clic su Aggiungi e selezionare Aggiungi nodi dai risultati di rilevamento dal menu di popup.

   Verrà visualizzata la schermata Aggiungi nodi dai risultati di rilevamento contenente un elenco dei nodi rilevati.

3. Dall'elenco Nodi rilevati, selezionare i nodi che si desidera aggiungere, quindi fare clic sulla freccia per aggiungerli all'elenco Nodi da proteggere. Al termine della procedura fare clic su Avanti.

   Nota: è possibile filtrare l'elenco in base al nome del nodo o del dominio per ridurre l'elenco.

4. (Facoltativo) Selezionare uno o più nodi e fare clic su Nascondi nodi selezionati per nascondere i nodi di cui non si desidera eseguire il backup.

5. (Facoltativo) Selezionare l'opzione Mostra nodi nascosti per visualizzare nuovamente i nodi nascosti per l'elenco Nodi rilevati. Per nascondere nuovamente i nodi, deselezionare l'opzione.

6. Nella schermata Credenziali nodo, immettere un nome utente e una password per il nodo che si desidera aggiungere. È possibile specificare credenziali globali oppure utilizzare credenziali specifiche per i nodi selezionati.

7. Fare clic su Fine.

I nodi verranno aggiunti.

Importa computer virtuali da vCenter/ESX

È inoltre possibile aggiungere nodi anche mediante l'opzione per l'importazione dei computer virtuali da server Center/ESX. Questa attività consente il rilevamento di tutti i computer virtuali in esecuzione sull'host specificato ma non esegue analisi automatiche periodiche. Se i computer virtuali vengono aggiunti in un secondo momento, sarà necessario ripetere l'operazione. In caso contrario, i computer virtuali non verranno riconosciuti.

Di seguito si riportano alcune distinzioni esistenti tra questa opzione e l'attività di rilevamento:

- I dettagli dei server ESX e vCenter devono essere immessi manualmente ogni volta che si utilizza questa opzione.
- È possibile aggiungere qualsiasi server specificato nell'elenco di rilevamento, senza la necessità di immettere le credenziali ogni volta.
- Tutti i computer virtuali disponibili vengono elencati ogni volta che si utilizza questa opzione. Vengono elencati anche i computer virtuali gestiti dall'applicazione.

Procedere come descritto di seguito:

1. Accedere all'applicazione.

   Fare clic su Nodo sulla barra di navigazione per aprire la schermata Nodo.

2. Dalla barra degli strumenti, fare clic su Aggiungi e selezionare Importa computer virtuali da Center/ESX dal menu di scelta rapida.

   Verrà visualizzata la finestra di dialogo Rileva nodi.

3. Completare i seguenti campi della schermata Rileva nodi:

   - Host vCenter/ESX

     Nota: se VMware Distributed Resource Scheduling (DRS) è in esecuzione nell'ambiente, si consiglia di specificare il nome host o l'indirizzo IP del sistema server vCenter durante l'operazione di importazione dei computer virtuali. Tale approccio consente di garantire il rilevamento dei computer virtuali in esecuzione nell'ambiente dell'utente e il corretto completamento dei backup dei computer virtuali DRS. Per evitare errori di backup durante lo spostamento di computer virtuali tra server ESX, si consiglia di non specificare il nome host o l'indirizzo IP del server ESX durante l'importazione dei computer virtuali.

     Per ulteriori informazioni su Distributed Resource Scheduling, consultare il sito Web di VMware.

   - Nome utente
   - Password
   - Porta
   - Protocollo

   Fare clic su Connetti e attendere il completamento dell'analisi.

4. (Facoltativo) Abilitare l'opzione Aggiungi server vCenter/ESX all'elenco di rilevamento automatico.
5. Fare clic su Avanti per aprire la finestra di dialogo Credenziali nodo.
6. Nella schermata Credenziali nodo, fornire un nome utente e una password globali per tutti i computer virtuali rilevati, quindi fare clic sull'opzione Applica. oppure fare clic su un computer virtuale per immettere credenziali specifiche.
7. Fare clic su Fine.

I computer virtuali selezionati verranno aggiunti al Gruppo nodi specificato.

Nota: CA ARCserve Central Host-Based VM Backup non è in grado di individuare i nomi host di computer virtuali in stato inattivo o su cui non sono installati gli strumenti VMware. In tal caso, dopo l'importazione dei nodi, il campo Nome host della schermata Nodo visualizzerà la dicitura Sconosciuto e il filtro Nome nodo (della schermata Nodo) non sarà in grado di filtrare nodi con nome Sconosciuto.

Aggiornamento dei nodi

CA ARCserve Central Host-Based VM Backup consente di aggiornare le informazioni relative ai nodi aggiunti precedentemente.

Procedere come descritto di seguito:

1. Accedere all'applicazione.

   Dalla barra di navigazione della pagina principale, fare clic su Nodo.

   Verrà visualizzata la schermata Nodo.

2. Dalla barra Gruppi, fare clic sul gruppo di Tutti i nodi oppure sul nome del gruppo contenente i nodi che si desidera aggiornare.

   I nodi associati al gruppo verranno visualizzati nell'elenco dei nodi.

3. Fare clic sul nodo da aggiornare, quindi fare clic con il tasto destro del mouse su Aggiorna nodo dal menu di scelta rapida.

   Verrà visualizzata la finestra di dialogo Aggiorna nodo.

   Nota: per aggiornare tutti i nodi del gruppo di nodi, fare clic con il tasto destro del mouse sul nome del gruppo di nodi e selezionare Aggiorna nodo dal menu di scelta rapida.

4. Aggiornare i dettagli del nodo.

   Nota: per aggiornare nodi multipli dell'Elenco nodi, selezionare i nodi desiderati, fare clic con il tasto destro del mouse su qualsiasi nodo, quindi selezionare Aggiorna nodo dal menu di scelta rapida. Il nome utente e la password coincidono per i nodi selezionati. L'opzione Specifica nuove credenziali e la casella di controllo Acquisisci controllo del nodo sono selezionate per impostazione predefinita. È possibile specificare un nuovo nome utente e una nuova password per i nodi selezionati ed imporre al server la gestione dei nodi specificati. Inoltre, è possibile selezionare l'opzione Usa le credenziali esistenti per applicare il nome utente e la password correnti. I campi vengono disattivati.

5. Fare clic su OK.

   La finestra di dialogo Aggiorna nodo verrà chiusa e i nodi verranno aggiornati.

Aggiornamento di nodi e criteri dopo la modifica del nome host del server CA ARCserve Central Applications

Quando viene eseguita una modifica del nome host del server CA ARCserve Central Host-Based VM Backup, è necessario aggiornare i nodi e i relativi criteri. Tali attività sono necessarie per mantenere la relazione fra il server e i nodi protetti da tale server. La tabella seguente descrive gli scenari possibili e le azioni applicabili a ciascuno scenario.

Scenario	Misura correttiva
Il nodo è stato aggiunto dopo la modifica del nome host del server CA ARCserve Central Host-Based VM Backup.	Non viene richiesta alcuna azione correttiva.
Il nodo è stato aggiunto prima della modifica del nome host del server CA ARCserve Central Host-Based VM Backup, senza applicare criteri.	Aggiornare il nodo. Per ulteriori informazioni, consultare la sezione Aggiornamento dei nodi (a pagina 49).
Il nodo è stato aggiunto prima della modifica del nome host del server CA ARCserve Central Host-Based VM Backup, applicando un criterio.	Applicare nuovamente il criterio. Per ulteriori informazioni, consultare la sezione Assegnazione di criteri a computer virtuali.

Eliminazione dei nodi

È possibile eliminare un nodo in qualsiasi momento.

Procedere come descritto di seguito:

1. Accedere all'applicazione.

   Fare clic su Nodo sulla barra di navigazione per aprire la schermata Nodo.

2. Dalla barra Gruppi, fare clic sul gruppo di Tutti i nodi oppure sul nome del gruppo contenente il nodo da eliminare.

   I nodi associati al gruppo verranno visualizzati nell'elenco dei nodi.

3. Selezionare i nodi che si desidera eliminare, quindi fare clic su Elimina sulla barra degli strumenti.

   Verrà visualizzato un messaggio di conferma.

4. Eseguire una delle seguenti operazioni:
   - Fare clic su Sì per eliminare il nodo.
   - Fare clic su No se non si desidera eliminare il nodo.

Opzioni del processo di unione

CA ARCserve Central Host-Based VM Backup consente di interrompere e riprendere i processi di unione per ogni nodo in qualsiasi momento. Il processo di interruzione e ripresa dei processi di unione non interessa i processi in corso.

Interruzione di un processo di unione su un nodo

CA ARCserve Central Host-Based VM Backup consente di interrompere un processo di unione su un nodo specifico.

Ad esempio, i processi di unione possono utilizzare risorse di sistema e causare un rallentamento dei processi di backup. Utilizzare l'opzione di interruzione per interrompere un processo di unione in corso in modo che i processi di backup in corso possano essere completati con la massima efficienza. Al completamento del backup, è possibile riprendere il processo di unione.

Procedere come descritto di seguito:

1. Dalla pagina principale di CA ARCserve Central Host-Based VM Backup, selezionare Criteri dalla barra di navigazione per accedere alla schermata Nodo.
2. Selezionare il gruppo di nodi contenente i nodi con processi di unione che si desidera interrompere.

   Verrà visualizzato un elenco di nodi per il gruppo selezionato.

3. Fare clic sui nodi contenenti i processi di unione che si desidera interrompere. Fare quindi clic con il tasto destro del mouse sui nodi selezionati, quindi selezionare Sospendi processo di unione dal menu di scelta rapida.

   Nota: per impostazione predefinita, l'opzione Sospendi processo di unione è disattivata. Quando il nodo esegue un processo di unione, in base a quanto indicato nella colonna Processo, l'opzione Sospendi processo di unione viene abilitata.

Il processo di unione del nodo selezionato viene interrotto e può essere verificato dalla pagina principale di CA ARCserve D2D.

Ripresa di un processo di unione su un nodo

CA ARCserve Central Host-Based VM Backup consente di riprendere processi di unione interrotti per un nodo specifico.

Procedere come descritto di seguito:

1. Dalla pagina principale di CA ARCserve Central Host-Based VM Backup, selezionare Criteri dalla barra di navigazione per accedere alla schermata Nodo.
2. Selezionare il gruppo di nodi contenente i nodi con processi di unione che si desidera riprendere.

   Verrà visualizzato un elenco di nodi per il gruppo selezionato.
3. Fare clic sui nodi con processi di unione interrotti o che si desidera riprendere. Fare quindi clic con il tasto destro del mouse sui nodi selezionati, quindi selezionare Riprendi processo di unione dal menu di scelta rapida.

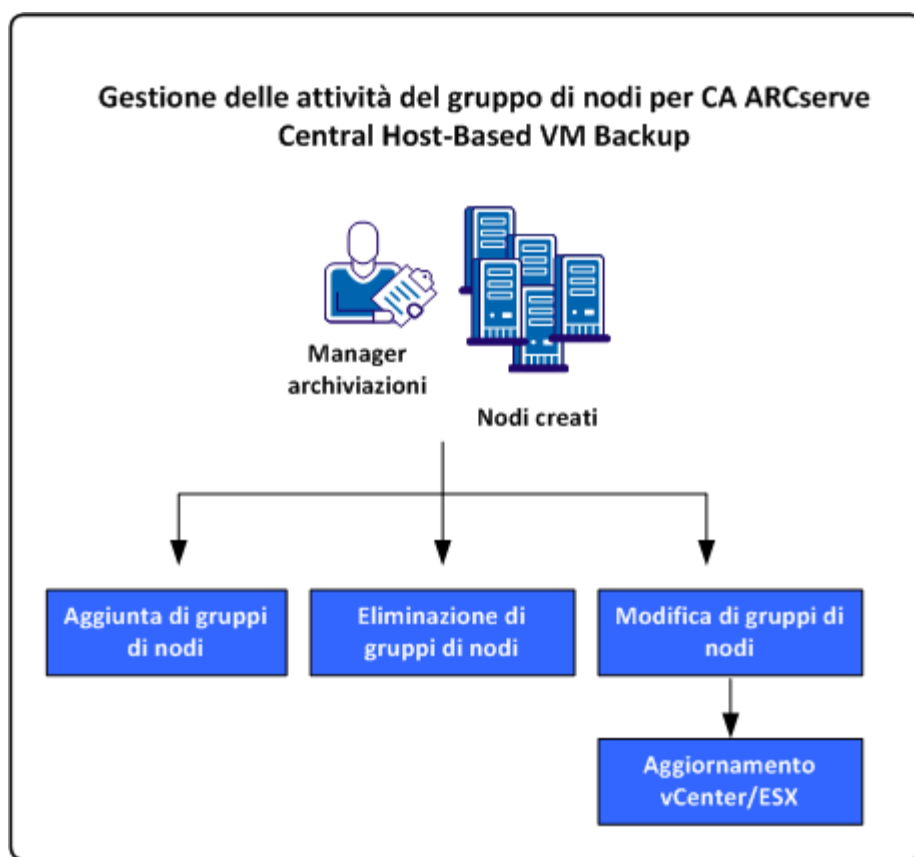
   Nota: l'opzione Riprendi processo di unione è abilitata se non è in esecuzione un processo di backup e i processi di unione sono interrotti.

Il processo di unione del nodo selezionato viene ripreso e può essere verificato dalla pagina principale di CA ARCserve D2D.

Modalità di gestione delle attività del gruppo nodi per CA ARCserve Central Host-Based VM Backup

CA ARCserve Central Host-Based VM Backup consente a un manager di archiviazione di proteggere numerosi computer virtuali contemporaneamente.

Avviare l'operazione mediante l'aggiunta di nodi. È possibile raggruppare i nodi per applicazione o per scopo. La creazione di gruppi di nodi consente di visualizzare facilmente l'ambiente dei computer virtuali. È possibile creare criteri di backup e assegnarli ai nodi al fine di semplificare la protezione dell'ambiente virtuale. Per ulteriori informazioni, consultare la sezione Modalità di gestione dei criteri per CA ARCserve Central Host-Based VM Backup (a pagina 75).

La seguente illustrazione descrive le attività che il Gruppo nodi consente di eseguire:

Il presente scenario descrive i seguenti argomenti:

Aggiunta di gruppi di nodi

Quando si esegue la prima importazione di un computer virtuale da un host ESX o vCenter, un nuovo gruppo di nodi viene aggiunto automaticamente.

I gruppi di nodi consentono di gestire un insieme di computer origine CA ARCserve D2D in base a caratteristiche comuni. Ad esempio, è possibile definire gruppi di nodi classificati in base al dipartimento che supportano: Contabilità, Marketing, Legale, Risorse umane, ecc.

L'applicazione contiene i seguenti gruppi di nodi:

- **Gruppi predefiniti:**
  - **Tutti i nodi** - Contiene tutti i nodi associati con l'applicazione.
  - **Nodi senza un gruppo** - Contiene tutti i nodi associati all'applicazione non assegnati a un gruppo di nodi.
  - **Nodi senza un criterio** - Contiene tutti i nodi associati all'applicazione che non dispongono di un criterio assegnato.
  - **SQL Server** - Contiene tutti i nodi associati con l'applicazione e che dispongono di Microsoft SQL Server.
  - **Exchange** - Contiene tutti i nodi associati con l'applicazione e che dispongono di Microsoft Exchange Server.

  Nota: i gruppi di nodi predefiniti non possono essere modificati o eliminati.
- **Gruppi personalizzati** - Contiene i gruppi di nodi personalizzati.
- **Gruppi vCenter/ESX**: se si aggiunge un nodo all'opzione Importa computer virtuali da vCenter/ESX, il nome del server vCenter/ESX viene aggiunto a tale gruppo.

Procedere come descritto di seguito:

1. Accedere all'applicazione.

   Dalla barra di navigazione della pagina principale, fare clic su Nodo per aprire la schermata Nodo.
2. Fare clic su Aggiungi nella barra degli strumenti Gruppo nodi.

   Si aprirà la finestra di dialogo Aggiungi gruppo e verranno visualizzati i nodi nell'elenco Nodi disponibili.
3. Specificare un Nome gruppo per il gruppo di nodi.

4. Completare i seguenti campi della finestra di dialogo Aggiungi gruppo:
   - **Gruppo:**selezionare il nome del gruppo contenente i nodi da assegnare.
   - **Filtro Nome nodo:** consente di filtrare i nodi disponibili in base a un criterio comune.

     Nota: il campo Nome nodo supporta l'uso di caratteri jolly.

     Ad esempio, Acc* consente di filtrare tutti i nodi il cui nome inizia per Acc. Per cancellare i risultati del filtro, fare clic su sul simbolo X del campo Filtro.
5. Per aggiungere nodi al gruppo di nodi, selezionare i nodi che si desidera aggiungere e fare clic sulla freccia destra singola.

   I nodi verranno spostati dall'elenco Nodi disponibili all'elenco Nodi selezionati e assegnati al gruppo di nodi.

   Nota: per selezionare e spostare tutti i nodi dal gruppo corrente, fare clic sulla freccia destra doppia.
6. Se si desidera spostare tutti i nodi dall'elenco Nodi selezionati all'elenco Nodi disponibili fare clic sulla freccia sinistra singola.

   Nota: per selezionare e spostare tutti i nodi dal gruppo corrente, fare clic sulla freccia sinistra doppia.
7. Fare clic su OK.

Il gruppo di nodi verrà aggiunto.

Eliminazione di gruppi di nodi

È possibile eliminare un gruppo di nodi in qualsiasi momento. Quando viene eliminato un gruppo aggiunto manualmente, i computer virtuali non vengono rimossi dall'applicazione. Tuttavia, se un gruppo creato automaticamente dal rilevamento di un server ESX o vCenter viene eliminato, il gruppo e tutti i computer virtuali verranno eliminati dall'applicazione.

L'applicazione consente di eliminare i gruppi di nodi creati.

Non è possibile eliminare i seguenti gruppi di nodi:

- **Tutti i nodi** - Contiene tutti i nodi associati con l'applicazione.
- **Nodi senza un gruppo** - Contiene tutti i nodi associati all'applicazione non assegnati a un gruppo di nodi.
- **Nodi senza un criterio** - Contiene tutti i nodi associati all'applicazione che non dispongono di un criterio assegnato.
- **SQL Server** - Contiene tutti i nodi associati con l'applicazione i cui nodi dispongono di Microsoft SQL Server.
- **Exchange** - Contiene tutti i nodi associati con l'applicazione i cui nodi dispongono di Microsoft Exchange Server.

Nota: il processo di eliminazione dei gruppi di nodi non comporta l'eliminazione dei singoli nodi dall'applicazione.

Procedere come descritto di seguito:

1. Accedere all'applicazione.

   Dalla barra di navigazione della pagina principale, fare clic su Nodo per aprire la schermata Nodo.

2. Fare clic sul gruppo di nodi da eliminare, quindi su Elimina nella barra degli strumenti Gruppo nodi.

   Verrà visualizzata una finestra di dialogo di conferma.

3. Se si è sicuri di voler eliminare il gruppo dei nodi, fare clic su Sì.

   Nota: fare clic su No se non si desidera cancellare il gruppo di nodi.

Il gruppo dei nodi viene eliminato.

Modifica di gruppi di nodi

L'applicazione consente di modificare i gruppi di nodi creati. È possibile aggiungere o rimuovere i nodi dai gruppi di nodi e modificare il nome dei gruppi.

Nota - I seguenti gruppi di nodi non possono essere modificati:

- **Tutti i nodi** - Contiene tutti i nodi associati con l'applicazione.
- **Nodi senza un gruppo** - Contiene tutti i nodi associati all'applicazione non assegnati a un gruppo di nodi.
- **Nodi senza un criterio** - Contiene tutti i nodi associati all'applicazione che non dispongono di un criterio assegnato.
- **SQL Server** - Contiene tutti i nodi associati con l'applicazione e che dispongono di Microsoft SQL Server.
- **Exchange** - Contiene tutti i nodi associati con l'applicazione e che dispongono di Microsoft SQL Server.

Procedere come descritto di seguito:

1. Accedere all'applicazione.

   Dalla barra di navigazione della pagina principale, fare clic su Nodo.

   Verrà visualizzata la schermata Nodo.

2. Fare clic sul gruppo di nodi da modificare, quindi selezionare Modifica nella barra degli strumenti Gruppo nodi.

   Verrà visualizzata la finestra di dialogo Modifica gruppo.

3. Per modificare il nome del gruppo, specificare un nuovo nome nel campo Nome gruppo.

4. Per aggiungere nodi al gruppo nodi, selezionare i nodi che si desidera aggiungere e fare clic sulla freccia destra.

   I nodi verranno spostati dall'elenco Nodi disponibili all'elenco Nodi selezionati e assegnati al gruppo di nodi.

   Nota: per spostare tutti i nodi dall'elenco Nodi disponibili all'elenco Nodi selezionati fare clic sulla freccia destra doppia.

5. Per rimuovere nodi dal gruppo di nodi, fare clic sulla freccia sinistra oppure sulla freccia sinistra doppia per rimuovere rispettivamente uno o tutti i nodi.

6. (Facoltativo) Per filtrare i nodi disponibili in base a criteri comuni, specificare un valore nel Filtro Nome nodo.

   Nota: il campo Filtro supporta l'uso di caratteri jolly.

   Ad esempio, Acc* consente di filtrare tutti i nodi il cui nome inizia per Acc. Per cancellare tutti i risultati del filtro, fare clic sul simbolo X del campo Filtro.

7. Fare clic su OK.

Il gruppo di nodi verrà modificato.

Aggiornamento dei dettagli dei server vCenter e ESX

CA ARCserve Central Host-Based VM Backup consente di aggiornare le informazioni relative ai server vCenter e ESC aggiunte precedentemente.

Procedere come descritto di seguito:

1. Dalla schermata Nodo, espandere la sezione Gruppi vCenter/ESX della barra Gruppi.
2. Selezionare il gruppo vCenter/ESX di cui si desidera eseguire l'aggiornamento delle informazioni del server, quindi fare clic con il tasto destro del mouse e selezionare Aggiorna vCenter/ESX.

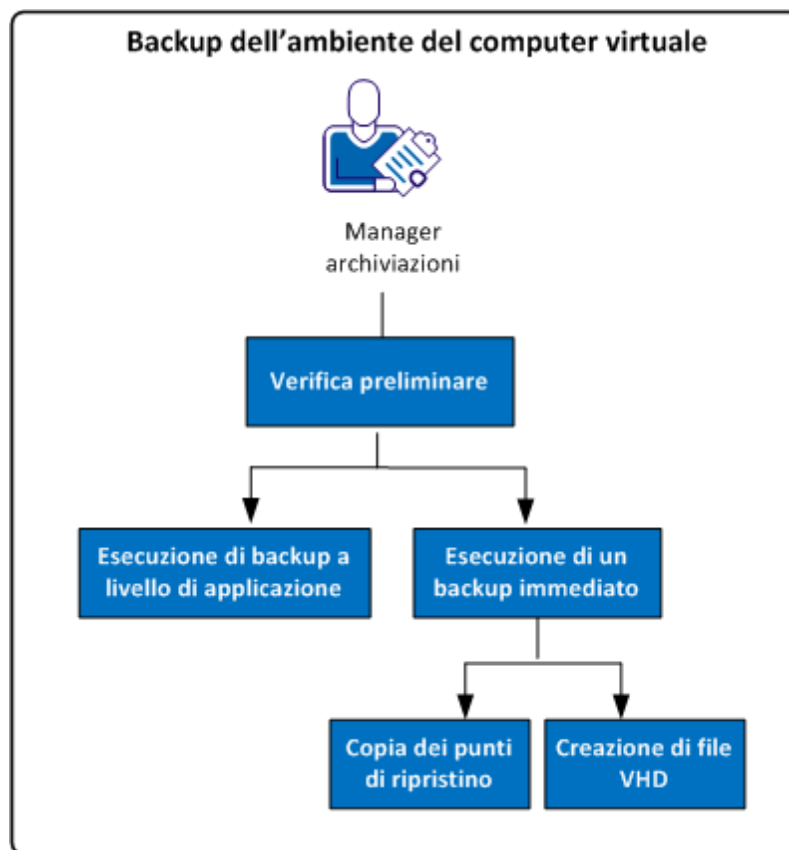
   Viene visualizzata la finestra di dialogo Aggiorna vCenter/ESX.

3. Aggiornare le informazioni relative al server vCenter/ESX.
4. Fare clic su OK (Salva/Applica).

   La finestra di dialogo Aggiorna vCenter/ESX viene chiusa e il nodo viene aggiornato.

Backup dell'ambiente del computer virtuale

Questo scenario descrive la procedura eseguita dal manager di archiviazione per il backup e la protezione di tutti i computer virtuali presenti nell'ambiente.

Il diagramma seguente illustra la modalità di backup dell'ambiente dei computer virtuali.

L'elenco seguente descrive i processi illustrati nel diagramma:

- Esecuzione di verifiche preliminari per i processi di backup (a pagina 60)
- Esecuzione di un backup immediato (a pagina 64)
  - Copia dei punti di ripristino di backup (a pagina 68)
  - Creazione di file VHD (a pagina 71)
- Esecuzione di backup a livello di applicazione (a pagina 71)

Esecuzione di verifiche preliminari per i processi di backup

CA ARCserve Central Host-Based VM Backup include un'utilità denominata Verifica preliminare che consente di eseguire controlli importanti su nodi specifici per rilevare eventuali condizioni che potrebbero determinare l'errore dei processi di backup. La Verifica preliminare viene eseguita automaticamente durante l'esecuzione delle azioni seguenti:

- Importazione di computer virtuali da un sistema server vCenter o ESX
- Aggiunta di nodi dai risultati del rilevamento
- Aggiornamento di un nodo

Inoltre, è possibile la funzionalità di Verifica preliminare può essere eseguita manualmente.

Procedere come descritto di seguito:

1. Accedere all'applicazione.

   Fare clic su Nodi nella barra di navigazione per aprire la schermata Nodi.

2. Effettuare una delle azioni seguenti per specificare i nodi per cui si desidera eseguire la verifica preliminare:

   - **Livello di nodo**: fare clic sul gruppo contenente i nodi per cui si desidera eseguire la verifica preliminare, quindi selezionare la casella di controllo accanto ai nodi. Fare clic con il tasto destro del mouse sui nodi e selezionare l'opzione Verifica preliminare dal menu di scelta rapida.
   - **Livello di gruppo**: fare clic con il tasto destro del mouse sul gruppo contenente i nodi, quindi selezionare Verifica preliminare.

   Verrà visualizzato il messaggio: Avvio della verifica preliminare del computer virtuale in corso.

3. Scorrere la pagina per visualizzare la colonna Stato verifica preliminare e visualizzare lo stato della verifica preliminare.

La tabella seguente descrive le verifiche eseguite dalla funzionalità di verifica preliminare:

Elemento	Descrizione
Funzionalità di traccia dei blocchi modificati	La funzionalità di traccia dei blocchi modificati consente di tenere traccia dei settori di disco modificati sul computer virtuale. Questa funzionalità consente di ridurre le dimensioni dei backup. Questo elemento verifica l'abilitazione della funzionalità di traccia dei blocchi modificati.
Strumenti VMware	Questo elemento verifica che gli strumenti VMware siano installati sui computer virtuale.

Elemento	Descrizione
Disco	Questo elemento verifica i dischi del computer virtuale.
Stato di alimentazione	Questo elemento verifica che il computer virtuale sia attivato.
Credenziali	Questo elemento verifica la validità delle credenziali utente.
Applicazioni	Questo elemento verifica l'installazione di Microsoft SQL Server e Microsoft Exchange Server.

Per ulteriori informazioni sulla risoluzione di errori e avvisi per i risultati della verifica preliminare, consultare la sezione Soluzioni per gli elementi di verifica preliminare (a pagina 61).

Soluzioni per gli elementi di verifica preliminare

Le tabelle seguenti descrivono le soluzioni per gli errori e avvisi contenuti nei risultati della verifica preliminare:

Funzionalità di traccia dei blocchi modificati

Stato	Messaggio	Soluzione
Avviso	La funzionalità di traccia dei blocchi modificati viene abilitata e contiene snapshot. Verrà applicato un backup completo del disco.	Per applicare il backup del blocco utilizzato, eseguire le seguenti operazioni: 1. Eliminare tutte le snapshot associate al computer virtuale. 2. Effettuare l'accesso al server proxy CA ARCserve Central Host-Based VM Backup. 3. Aprire l'editor del Registro di sistema e cercare la seguente chiave: HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA ARCserve D2D\AFBackupDll\<VM-InstanceUUID> **Nota**: Sostituire <VM-InstanceUUID> con il valore UUID del computer virtuale su cui si sta verificando l'errore della funzionalità di traccia dei blocchi modificati. Il valore può essere reperito nell'URL del computer virtuale utilizzato durante la connessione a CA ARCserve D2D. 4. Impostare la chiave del Registro di sistema su "full disk backupForFullBackup"=0. 5. Creare/impostare il registro di sistema su ResetCBT=1. 6. Inoltrare il processo di backup.

Strumenti VMware

Stato	Messaggio	Soluzione
Avviso	Non aggiornato.	Installare la versione più recente degli strumenti VMware.
Avviso	Non installato o non in esecuzione.	Installare la versione più recente degli strumenti VMware e verificarne l'esecuzione.

Disco

Stato	Messaggio	Soluzione
Errore	Le snapshot di computer virtuale non sono supportate dal computer virtuale in quanto il controller SCSI è stato configurato per la configurazione della condivisione di bus.	Utilizzare CA ARCserve Central Protection Manager o CA ARCserve D2D per eseguire il backup del computer virtuale.
Avviso	Non verrà eseguito il backup del disco fisico di mapping della periferica non formattata.	Utilizzare CA ARCserve Central Protection Manager o CA ARCserve D2D per eseguire il backup del computer virtuale.
Avviso	Il backup del disco virtuale di mapping della periferica non formattata verrà eseguito come disco completo.	Utilizzare CA ARCserve Central Protection Manager o CA ARCserve D2D per eseguire il backup del computer virtuale.
Avviso	Non verrà eseguito il backup del disco indipendente.	Utilizzare CA ARCserve Central Protection Manager o CA ARCserve D2D per eseguire il backup del computer virtuale.
Avviso	Verrà eseguito il backup del disco sull'archivio dati NFS come disco completo.	Utilizzare CA ARCserve Central Protection Manager o CA ARCserve D2D per eseguire il backup del computer virtuale.

Stato di alimentazione

Stato	Messaggio	Soluzione
Avviso	Disattivato	Avviare il computer virtuale.
Avviso	Sospeso	Avviare il computer virtuale.

Credenziali

Stato	Messaggio	Soluzione
Avviso	Credenziali non corrette.	Specificare credenziali utente valide.
Avviso	Non fornito.	Specificare credenziali utente valide.

Applicazioni

Stato	Messaggio	Soluzione
Avviso	Il ripristino a livello di applicazione non è supportato in quanto il computer virtuale contiene dischi IDE.	Utilizzare CA ARCserve Central Protection Manager o CA ARCserve D2D per eseguire il backup dei dati di Microsoft SQL Server e di Exchange Server.
Avviso	VMware VIX non è installato sul server host.	Eseguire il download di VIX dal sito Web di VMware e installarlo sul server host di CA ARCserve Central Applications.
Avviso	La versione di VMware VIX sul server CA ARCserve Central Host-Based VM Backup non è aggiornata.	Eseguire il download di VIX dal sito Web di VMware e installarlo sul server host di CA ARCserve Central Applications.
Avviso	Il ripristino di livello di applicazione non è supportato in quanto il supporto del server ESX non è disponibile.	Aggiornare il server ESX alla versione 4.1 o successiva oppure utilizzare CA ARCserve Central Protection Manager o CA ARCserve D2D per eseguire il backup dei dati di Microsoft SQL Server e di Exchange Server.
Avviso	Il ripristino a livello di applicazione non è supportato poiché il numero di slot SCSI disponibili non è sufficiente.	Utilizzare CA ARCserve Central Protection Manager o CA ARCserve D2D per eseguire il backup dei dati di Microsoft SQL Server e di Exchange Server.
Avviso	poiché l'origine risiede in un disco dinamico. Il ripristino a livello di applicazione non è supportato	Utilizzare CA ARCserve Central Protection Manager o CA ARCserve D2D per eseguire il backup dei dati di Microsoft SQL Server e di Exchange Server. **Nota**: VMware non supporta la disattivazione a livello di applicazione dei computer virtuali Windows Server 2008 o versioni successive con dischi dinamici in esecuzione su ESX Server 4.1 o versioni successive.

Stato	Messaggio	Soluzione
Avviso	Impossibile acquisire le informazioni relative all'applicazione. È possibile che i backup a livello di applicazione non vengano eseguiti correttamente.	Fornire le credenziali predefinite o di amministratore dominio per accedere al sistema operativo guest del computer virtuale. A causa di una limitazione di VMware, il backup è supportato soltanto su computer virtuali in esecuzione su un server ESX con licenza acquistata. Il backup non viene supportato su un server ESXi con una licenza libera.
Avviso	Il ripristino a livello di applicazione non è supportato su sistemi con spazi di archiviazione attivati. È possibile eseguire unicamente il ripristino dell'intero computer virtuale.	Utilizzare CA ARCserve Central Protection Manager o CA ARCserve D2D per eseguire il backup dei dati di Microsoft SQL Server e di Microsoft Exchange Server.

Esecuzione di un backup immediato

In genere, i backup vengono eseguiti automaticamente e vengono controllati attraverso le impostazioni di pianificazione. Ad ogni modo, potrebbe essere necessario eseguire un backup ad hoc immediato (completo, incrementale o di verifica).

Il backup ad hoc viene eseguito a seconda delle esigenze, e non viene pianificato come parte di un piano di backup. Ad esempio, se sono stati pianificati backup completi, incrementali e di verifica e si desidera apportare modifiche sostanziali al computer, sarà necessario eseguire un backup ad hoc immediato senza attendere l'esecuzione del backup pianificato successivo.

Un backup ad hoc consente inoltre di aggiungere un punto di ripristino personalizzato (non pianificato) per tornare al punti precedente specificato, in qualsiasi momento.. Ad esempio, se si procede all'installazione di una patch o di un service pack e, successivamente, si rileva che tale installazione influenza le prestazioni del computer, potrebbe essere necessario eseguire un ripristino utilizzando la sessione di backup ad hoc precedente all'installazione.

Procedere come descritto di seguito:

1. Accedere all'applicazione.
2. Dalla barra di navigazione della pagina principale, fare clic su Nodo per aprire la schermata Nodo.

3. Eseguire una delle azioni seguenti per specificare i nodi di cui si desidera eseguire il backup:
   - **Livello di nodo:** fare clic sul gruppo contenente i nodi di cui si desidera eseguire il backup e selezionare la casella di controllo corrispondente.
   - **Livello di gruppo:** fare clic sul gruppo contenente i nodi di cui si desidera eseguire il backup.
4. Effettuare quindi una delle azioni seguenti per eseguire il backup del nodo:
   - Fare clic su Backup dalla barra degli strumenti.
   - Fare clic con il tasto destro del mouse sul gruppo o sui nodi selezionati, quindi fare clic sul Esegui backup dal menu di scelta rapida.

5. Nella finestra di dialogo Esecuzione di un backup immediato, specificare il tipo di backup selezionando uno dei tipi seguenti:

   - **Backup completo -** Avvia un backup completo di tutto il computer o dei volumi selezionati.
   - **Backup incrementale -** Avvia un backup incrementale del computer. Un backup incrementale esegue il backup solo dei blocchi modificati dopo l'ultimo backup.

     Nota: i backup incrementali presentano il vantaggio di essere particolarmente rapidi e di generare immagini di backup di dimensioni molto ridotte. Questa modalità di esecuzione backup è ottimale.
   - **Backup di verifica -** Avvia un backup di verifica del computer analizzando il backup più recente di ciascun singolo blocco e ne confronta il contenuto e le informazioni con l'origine iniziale. Questo confronto consente di verificare che le informazioni corrispondenti all'origine siano contenute nel blocco di backup più recente. Se l'immagine di backup di un determinato blocco non corrisponde all'origine, CA ARCserve D2D aggiornerà (risincronizzerà) il backup di tale blocco. L'esecuzione di un backup di verifica presenta i seguenti vantaggi e svantaggi:
     - Vantaggio: questo tipo di backup genera un'immagine di backup con dimensioni ridotte rispetto al backup completo, in quanto esegue solamente il backup dei blocchi modificati, ovvero dei blocchi che non corrispondono al backup più recente.
     - Svantaggio: la velocità del tempo di backup è ridotta in quanto i blocchi di backup originali vengono confrontati con i blocchi di backup più recenti.

   Nota: se si aggiunge un nuovo volume all'origine di backup, il volume appena aggiunto verrà sottoposto a un backup completo, indipendentemente dal metodo di backup generale utilizzato.

6. (Facoltativo) Specificare un nome di backup e fare clic su OK. Se non viene specificato un nome, il backup verrà utilizzato il nome predefinito Customized/Full/Incremental/Verify Backup.

Verrà visualizzata una finestra di dialogo di conferma e il tipo di backup selezionato verrà avviato automaticamente.

Tenere presenti le seguenti considerazioni:

- Tutti i valori specificati nelle finestre di dialogo Criterio verranno applicati al processo.
- In caso di errore di un processo di backup (ad hoc) personalizzato, non verrà creato alcun processo di composizione. I processi di riparazione vengono creati solo in caso di errore di processi pianificati.
- CA ARCserve Central Host-Based VM Backup applica i seguenti processi di backup in base all'ordine di priorità:
  - Completo
  - Verifica
  - Incrementale

  Le condizioni seguenti si verificano con l'avvio dell'operazione Esegui backup e un processo è in attesa nella coda:
  - Quando viene inviato un processo di backup completo ed è presente un processo Backup di verifica nella coda, il processo di backup completo sovrascriverà il processo nella coda.
  - Quando viene inviato un processo di backup completo ed è presente un processo Backup incrementale nella coda, il processo di backup completo sovrascriverà il processo nella coda.
  - Quando viene inviato un processo di backup completo ed è presente un processo Backup incrementale nella coda, il processo del backup di verifica sovrascriverà il processo nella coda.
  - Quando viene inviato un processo Backup di verifica ed è presente un processo di backup completo nella coda, il processo Backup di verifica viene ignorato.
  - Quando viene inviato un processo di backup incrementale ed è presente un processo di backup completo nella coda, il processo Backup incrementale viene ignorato.
  - Quando viene inviato un processo di backup incrementale ed è presente un processo di backup di verifica nella coda, il processo Backup incrementale viene ignorato.

Copia punti di ripristino

Quando un backup di CA ARCserve D2D viene completato con successo, viene creata un'immagine snapshot temporizzata del backup. L'insieme dei punti di ripristino consente di individuare e specificare un'immagine di backup da copiare. Per proteggere i backup, procedere nel seguente modo:

- Copiare/esportare le informazioni del punto di ripristino per eseguirne l'archiviazione protetta remota nel caso in cui si verifichi un errore irrecuperabile.
- Salvare i punti di ripristino in più percorsi.
- Consolidare i backup nel caso in cui la destinazione sia completa e si desideri conservare tutti i punti di ripristino.

Quando un punto di ripristino viene selezionato per la copia, vengono acquisiti anche tutti i blocchi di backup precedenti necessari per ricreare un'immagine di backup completa e recente.

Procedere come descritto di seguito:

1. Accedere all'applicazione.

   Fare clic su Nodo sulla barra di navigazione per aprire la schermata Nodo.

2. Dall'elenco Gruppi, fare clic su Tutti i nodi oppure sul gruppo contenente il nodo CA ARCserve D2D che include i punti di ripristino che si desidera copiare.

   Nell'elenco dei nodi verranno visualizzati tutti i nodi associati al gruppo specificato.

3. Individuare e fare clic sul nodo a cui si desidera accedere, quindi su Accesso a D2D dal menu di scelta rapida.

   Verrà visualizzata la pagina principale del nodo di CA ARCserve D2D.

   Nota: verificare che le opzioni popup della finestra del browser siano abilitate.

4. Dalla pagina principale di CA ARCserve D2D, selezionare Copia punto di ripristino.

   Verrà visualizzata la finestra di dialogo Copia punto di ripristino.

5. Nel campo Posizione di backup, specificare l'origine di backup. È possibile specificare una posizione oppure individuare il percorso di archiviazione delle immagini di backup. Per verificare la connessione al percorso specificato, fare clic sull'icona della freccia verde. Se necessario, immettere le credenziali Nome utente e Password per poter accedere al percorso.

6. Nel campo Computer virtuale, fare clic sull'elenco a discesa accanto a Seleziona computer virtuale per specificare il computer virtuale contenente i punti di ripristino che si desidera copiare.

   La visualizzazione calendario evidenzia tutte le date che contengono punti di ripristino per l'origine di backup specificata all'interno nel periodo di tempo visualizzato.

7. Specificare il punto di ripristino da copiare.

   a. Nel calendario, selezionare la data dell'immagine di backup che si desidera copiare.

      Verranno visualizzati, quindi, i punti di ripristino associati alla data, unitamente all'ora di backup, al tipo di backup eseguito e al nome del backup.

      Nota: l'icona di un orologio con lucchetto indica che il punto di ripristino contiene informazioni crittografate e richiede una password per il ripristino.

   b. Selezionare il punto di ripristino che si desidera copiare.

      Verrà visualizzato il contenuto del backup (eventuali applicazioni incluse) per il punto di ripristino selezionato.

8. Fare clic su Avanti.

   Viene visualizzata la finestra di dialogo Opzioni di copia.

   Nota: questa finestra di dialogo contiene due campi password. Il campo Password contiene la password di decrittografia della sessione di origine, mentre il campo Crittografia viene utilizzato per la crittografia della sessione di destinazione.

   a. Se il punto di ripristino esportato è stato precedentemente crittografato, verrà richiesta una password.

      - Se il punto di ripristino esportato è una sessione di backup dello stesso computer che esegue il processo di copia del punto di ripristino, la password di crittografia verrà salvata e popolata automaticamente.
      - Se il punto di ripristino esportato è una sessione di backup di un altro computer, verrà richiesta una password di crittografia.

   b. Selezionare la destinazione.

      È possibile specificare una posizione o individuare il percorso di archiviazione della copia del punto di ripristino selezionato. Per verificare la connessione al percorso specificato, fare clic sull'icona della freccia verde. Se necessario, immettere o modificare il nome utente e la password.

c. Selezionare il livello di compressione desiderato.

Nota: il livello di compressione specificato per il backup è indipendente dal livello di compressione della copia. Ad esempio, se il livello di compressione della destinazione di backup è impostato su Standard, al momento di invio del processo di copia è possibile modificare la compressione in Nessuna compressione o Compressione massima.

La compressione consente solitamente di ridurre l'utilizzo dello spazio su disco. Tuttavia, può avere un effetto inverso e ridurre la velocità di backup a causa dell'aumento dell'utilizzo della CPU.

Le opzioni disponibili sono:

- **Nessuna compressione** - Non viene eseguito alcun tipo di compressione. I file sono di tipo VHD. L'opzione determina un utilizzo minimo della CPU (velocità massima) e un utilizzo massimo dello spazio su disco per la creazione dell'immagine di backup.
- **Compressione standard** - Comporta un livello medio di compressione. Questa opzione fornisce un buon bilanciamento tra l'utilizzo della CPU e dello spazio su disco. Si tratta dell'impostazione predefinita.
- **Compressione massima** - Verrà applicata la massima compressione. L'opzione implica un utilizzo massimo di CPU (velocità minima) ma utilizza anche una quantità minore di spazio su disco per l'immagine di backup.

Osservare il seguente esempio:

- Se l'immagine di backup contiene dati non comprimibili (come immagini JPG, file .zip), lo spazio di archiviazione aggiuntivo viene utilizzato per gestire tali dati. Di conseguenza, se si seleziona una qualsiasi opzione di compressione e il backup contiene dati non comprimibili, l'utilizzo di spazio su disco potrebbe aumentare.
- Modificando il livello di compressione da Nessuna compressione a Compressione standard o Compressione massima, oppure da Compressione standard o Compressione massima a Nessuna compressione, il primo backup eseguito dopo la modifica del livello di compressione diventa automaticamente un backup completo. Dopo l'esecuzione del primo backup completo, tutti i backup successivi (completo, incrementale o di verifica) verranno eseguiti come pianificati.

d. Se si desidera crittografare il punto di ripristino copiato, immettere le seguenti informazioni:

È possibile modificare, aggiungere o rimuovere la crittografia per il punto di ripristino copiato.

- Selezionare il tipo di algoritmo di crittografia da utilizzare per la copia.

  Le opzioni di formato disponibili sono Nessuna crittografia, AES-128, AES-192 e AES-256.
- Specificare e confermare una password di crittografia.

9. Fare clic su Crea una copia.

   Viene visualizzata una finestra di notifica dello stato e il processo di copia per il tipo di punto di ripristino selezionato viene avviato immediatamente.

   Nota: CA ARCserve D2D consente di eseguire un solo processo di copia del punto di ripristino alla volta.

   L'immagine del punto di ripristino viene copiata dall'origine di backup alla destinazione di copia.

Creazione di file VHD da CA ARCserve Central Host-Based VM Backup

Questa procedura di CA ARCserve D2D consente di creare un file VHD (Virtual Hard Disk) dal punto di ripristino creato dopo ogni backup completato. Per ulteriori informazioni, consultare l'Appendice di CA ARCserve D2D.

Procedere come descritto di seguito:

1. Eseguire la procedura Copia punti di ripristino (a pagina 68).
2. Quando la copia è terminata, selezionare la destinazione specificata e accedere all'host di CA ARCserve D2D.
3. Aprire la cartella, VStore\S0000000001.
4. Individuare tutti i file con estensione D2D e modificarne l'estensione in VHD. Dopo aver rinominato tutti i file, sarà possibile utilizzarli come normali file VHD.

Esecuzione di backup a livello di applicazione

In genere, non è necessario eseguire operazioni speciali per la protezione dei sistemi Microsoft Exchange o SQL server.

Per eseguire un backup di applicazione completo, verificare le condizioni seguenti:

- Tutti i writer delle applicazioni sono in uno stato stabile. Utilizzare *vssadmin* per visualizzare lo stato del writer.
- Tutti i database di cui è stato eseguito il backup presentano uno stato integro. Ad esempio, per SQL server, verificare che lo stato del database non corrisponda a *Ripristino in corso*.

Inoltre, è possibile troncare separatamente i registri delle transazioni per i server SQL ed Exchange.

Nota: se si esegue l'aggiornamento di un server ESX, prima di procedere a un backup a livello di applicazione sarà necessario aggiornare gli strumenti VMware del sistema operativo guest per evitare errori dovuti al mancato aggiornamento.

Esecuzione di backup di disco completi contenenti soltanto dati di blocco utilizzati

Il recupero dei dati di blocco utilizzati dopo l'esecuzione di backup completi del disco consente di ridurre la finestra di backup e di diminuire l'utilizzo di spazio sulla destinazione di backup.

Nota: a causa di limitazione di VMware, i blocchi utilizzati non possono essere recuperati dai computer virtuali in cui sono presenti snapshot del punto di ripristino. In tali casi viene eseguito un backup completo del disco sul computer virtuale.

Dopo l'invio di un backup di disco completo, eseguire le seguenti operazioni per recuperare i dati di blocco utilizzati:

1. Eliminare tutte le snapshot associate al computer virtuale.
2. Accedere al computer virtuale CA ARCserve Central Host-Based VM Backup.
3. Aprire l'editor del Registro di sistema e cercare la seguente chiave:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA ARCserve D2D\AFBackupDll\VM_InstanceUUID
   ```

4. Impostare la chiave di registro "full disk backupForFullBackup" su 0.
5. Creare o impostare il registro di sistema "ResetCBT" su 1.
6. Inoltrare il processo di backup.

Visualizzazione delle informazioni sullo stato del processo,

CA ARCserve Central Virtual Standby converte i punti di ripristino di CA ARCserve D2D in snapshot del punto di ripristino. È possibile visualizzare le informazioni di stato relative ai processi di backup dei computer virtuali basato sull'host in corso.

nonché visualizzare informazioni dettagliate sul processo. nonché interrompere il processo corrente.

Procedere come descritto di seguito:

1. Accedere all'applicazione.
2. Nella barra di navigazione, fare clic su Nodo per visualizzare la schermata corrispondente.
3. Se sono presenti processi di backup dei computer virtuali basato sull'host in corso, la fase del processo viene visualizzata nel campo Processo, come illustrato nell'immagine seguente:

	Nome nodo	Criterio	Processo
	w2k8r2jvp2	Nuovo criterio	Avvio del backup in cor

4. Fare clic sulla fase per aprire la finestra di dialogo Monitoraggio dello stato di backup.

   Nota: per informazioni sui campi visualizzati nel monitoraggio dello stato di backup, consultare la sezione Monitoraggio dello stato di backup (a pagina 73).

5. Selezionare una delle seguenti opzioni:

   - Fare clic su Chiudi per chiudere la finestra di dialogo Monitoraggio dello stato di backup.
   - Fare clic su Annulla per interrompere il processo corrente.

     Nota: la finestra di dialogo Monitoraggio dello stato di backup verrà chiusa qualche secondo dopo aver selezionato Annulla.

Ulteriori informazioni:

Visualizzazione delle informazioni sullo stato del processo, (a pagina 72)

Attività di monitoraggio di backup dei computer virtuali basato sull'host

È possibile visualizzare lo stato dei backup del computer virtuale nella schermata Nodo. Individuare il nodo che presenta un processo in corso utilizzando il campo Processo, quindi fare clic sul collegamento per visualizzare la finestra di dialogo.

I backup del computer virtuale vengono eseguiti in due fasi. In primo luogo, viene eseguito il backup dei dischi rigidi virtuali. Se questa operazione viene completata correttamente, viene generato il catalogo. Il catalogo consente di ripristinare file e cartelle, nonché l'intero computer virtuale.

Il computer di monitoraggio visualizza le seguenti informazioni sullo stato del processo di backup in tempo reale:

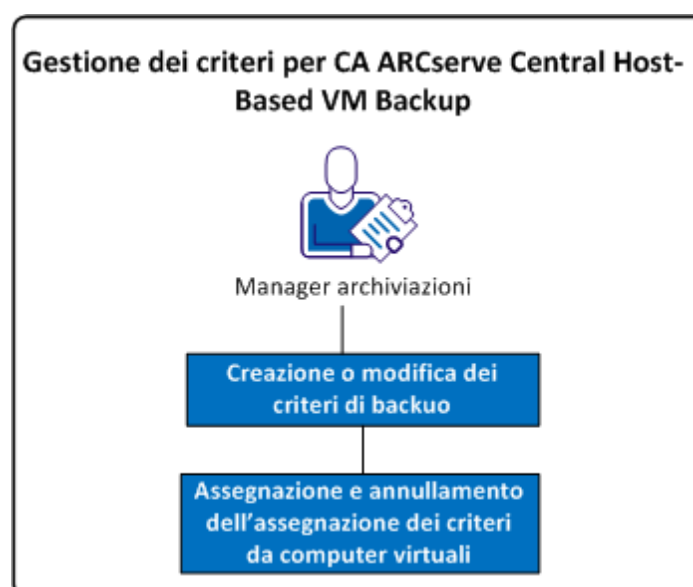
- **Fase - (Monitoraggio di backup e cataloghi)** Visualizza il punto corrente del processo, rappresentato dalla parte ombreggiata della barra di stato.
- **Ora di inizio - (Monitoraggio di backup e cataloghi)** Visualizza la data e l'ora di avvio dell'operazione di backup, in base alla configurazione del criterio.
- **Tempo trascorso - (Monitoraggio di backup e cataloghi)** Visualizza la differenza tra l'ora di inizio e l'ora corrente.
- **Tempo residuo stimato - (Solo monitoraggio di backup)** Visualizza il tempo stimato per il completamento del processo.
- **Elaborazione** - **(Solo monitoraggio di cataloghi)** Visualizza la lettera dell'unità o l'applicazione per la quale viene generato il catalogo.

- **Spazio recuperato mediante la compressione - (Solo monitoraggio di backup)** Visualizza lo spazio su disco recuperato nel caso in cui sia stata specificata la compressione nel criterio dell'operazione di backup.
- **Livello di Compressione** - **(Solo monitoraggio di backup)** Visualizza il tipo di compressione utilizzato per i backup. Le opzioni disponibili sono: Nessuna compressione, Compressione standard (impostazione predefinita) o Compressione massima.
- **Crittografia - (Solo monitoraggio di backup)** Visualizza il metodo di crittografia selezionato al momento della configurazione del processo di backup.
- **Limite di velocità di scrittura - (Solo monitoraggio di backup)** Visualizza il valore se il limite di velocità del backup è stato impostato nella schermata Impostazioni di protezione del criterio di backup.
- **Velocità di scrittura - (Solo monitoraggio di backup)** Visualizza la velocità di scrittura effettiva in megabyte/minuto.
- **Velocità di lettura - (Solo monitoraggio di backup)** Visualizza la velocità di lettura effettiva in megabyte/minuto.

Modalità di gestione dei criteri per CA ARCserve Central Host-Based VM Backup

I criteri di backup definiscono in che modalità e quando eseguire il backup dei nodi importati dal server vCenter/ESX. I responsabili della gestione archiviazione possono creare e modificare i criteri di backup, quindi assegnarli o annullarne l'assegnazione ai nodi.

Nota: è possibile assegnare un criterio a uno o a più nodi. Tuttavia, non è possibile assegnare uno o più criteri a un nodo.

Il seguente diagramma illustra il processo di amministrazione dei criteri di backup.

L'elenco seguente descrive i processi illustrati nel diagramma:

- Creazione di criteri di backup. (a pagina 76)
- Modifica dei criteri di backup (a pagina 80)
- Assegnazione e annullamento assegnazione nodi da criteri di backup. (a pagina 83)

Creazione di criteri di backup.

Il processo di creazione di criteri di backup utilizza l'interfaccia di CA ARCserve D2D per la configurazione delle impostazioni di backup con alcune distinzioni. È possibile creare criteri in base a esigenze di backup simili (ad esempio, per applicazione installata o per pianificazione).

La seguente procedura riassume le fasi necessarie per la creazione di un criterio del processo di backup CA ARCserve D2D semplice. Per informazioni complete sulla creazione di criteri di backup di CA ARCserve D2D, consultare le sezioni corrispondenti dell'Appendice.

Nota: durante un'operazione di backup host-based, viene visualizzato il seguente messaggio se si utilizza hotadd come modalità di trasporto:

```
È necessario formattare il disco nell'unità <letteraUnità> prima di poterlo
utilizzare. Formattare?
```

Fare clic su Annulla per ignorare questo messaggio. Il messaggio viene visualizzato quando il sistema operativo rileva che un disco rigido virtuale è stato aggiunto al server proxy di backup. Il sistema operativo suppone che il disco rigido virtuale sia una nuova periferica per la quale è richiesta la formattazione. Nel caso in cui l'opzione Formatta disco venga selezionata per errore, non verrà eseguita alcuna operazione in quanto il disco rigido virtuale è disponibile in sola lettura.

Procedere come descritto di seguito:

1. Accedere all'applicazione.

   Fare clic su Criteri nella barra di navigazione per accedere alla schermata Criteri.

2. Fare clic sul pulsante Nuovo della barra degli strumenti per visualizzare la finestra di dialogo Nuovo criterio.

3. Immettere un nome che descriva appropriatamente il criterio.

4. Dalla scheda Impostazioni di backup, fare clic su Impostazioni di protezione e specificare le seguenti informazioni:

   - **Destinazione di backup** - Specificare un volume locale o una cartella condivisa remota per il salvataggio delle sessioni di backup.
   - **Proxy di backup del computer virtuale CA ARCserve D2D** - Specificare il nome host o l'indirizzo IP del server su cui è stato installato CA ARCserve D2D. Se CA ARCserve D2D non è già stato installato, è possibile utilizzare CA ARCserve Central Protection Manager per la sua distribuzione. Fornire le credenziali appropriate per il server. Il valore predefinito per il numero di porta corrisponde a 8014. Se questo valore predefinito è stato modificato durante l'installazione di CA ARCserve D2D, specificare il numero di porta corretto.
   - **Impostazioni di memorizzazione** - È possibile impostare il criterio di memorizzazione in base al numero di punti di ripristino da memorizzare (unione delle sessioni) o al numero di set di ripristino da memorizzare (elimina i set di ripristino e disattiva i backup incrementali infiniti). L'opzione predefinita corrisponde a Mantieni i punti di ripristino. Per ulteriori informazioni, consultare la sezione Definizione delle impostazioni di protezione della Guida per l'utente di CA ARCserve Central Protection Manager.
   - **Compressione** - Selezionare un livello di compressione. Il valore predefinito è Standard. È possibile selezionare i valori Nessuna compressione o Compressione massima.
   - **Crittografia** - Selezionare un livello di crittografia. Il valore predefinito corrisponde a Nessuna crittografia. Se si specifica un livello di crittografia, sarà necessario immettere una password di crittografia per il ripristino dei dati crittografati.
   - **Limite di velocità del backup** - Immettere la percentuale di scrittura dei backup su disco. Ridurre la percentuale per diminuire il carico di CPU o di rete. Tenere presente che l'operazione aumenta la durata del processo di backup. Questa opzione è disattivata per impostazione predefinita.

5. Fare clic su Pianificazione e completare le seguenti informazioni:

   - **Data e ora di inizio** - Specificare la data e l'ora di inizio desiderate per l'avvio dei processi di backup.
   - **Backup incrementale** - Definire una pianificazione ripetuta per i processi di backup incrementale. Il valore predefinito è impostato sulla ripetizione dei backup incrementali una volta al giorno.
   - **Backup completo** - Definire una pianificazione ripetuta per i processi di backup completo. Per impostazione predefinita, il valore è impostato per non essere mai ripetuto.
   - **Backup di verifica** - Definire una pianificazione ripetuta per i processi di backup di verifica. Per impostazione predefinita, il valore è impostato per non essere mai ripetuto.

6. Fare clic su Avanzate e completare le seguenti informazioni:
   - **Tronca registro** - Consente di abilitare le seguenti opzioni, nel caso in cui si desideri troncare i file di registro dell'applicazione.
     - **SQL Server** - Specificare una pianificazione di troncamento giornaliera, settimanale o mensile.
     - **Exchange Server** - Specificare una pianificazione di troncamento giornaliera, settimanale o mensile.
   - **Riserva spazio sulla destinazione** -Specifica la percentuale di spazio da riservare per l'esecuzione di un backup. Tale valore di spazio viene riservato immediatamente sulla destinazione prima che il backup avvii la scrittura dei dati, consentendo di aumentare la velocità di backup.
   - **Cataloghi** - Selezionare l'opzione di generazione del catalogo di file system per l'esecuzione di ricerche più veloci dopo il backup e ridurre i tempi di attesa durante la ricerca.

     Se questa opzione non è selezionata, è possibile eseguire immediatamente i ripristini dopo il backup senza dovere attendere il completamento del processo di catalogo. Per impostazione predefinita, l'opzione non è abilitata. Tenere presenti le seguenti considerazioni:
     - Se viene generato un catalogo di file system per ciascun processo di backup, lo spazio necessario per l'archiviazione dei file di metadati e di catalogo sarà maggiore, così come l'utilizzo della CPU. Inoltre, se l'origine di backup contiene un numero elevato di file, il processo di generazione di un catalogo potrebbe richiedere tempi lunghi.
     - Se i volumi di ReFS vengono selezionati come origine di backup, non sarà possibile eseguire la generazione dei cataloghi. In tal caso, verrà visualizzato un messaggio di avviso che informa l'utente della condizione.

7. Fare clic su Impostazioni pre/post backup e specificare i comandi desiderati di pre o post backup. Se necessario, immettere le credenziali necessarie:
   - **Esegui un comando prima dell'avvio del backup** - Immettere il comando di script da eseguire prima dell'avvio del processo di backup.
   - **Sul codice di uscita** - Abilitare questa opzione se si desidera attivare il comando di script su un codice di uscita specifico.
   - **Esegui processo** - Se l'opzione è selezionata, il software procede con l'esecuzione del processo nel caso in cui il codice di uscita specificato venga restituito.
   - **Interrompi processo** - Se l'opzione è selezionata, il software interrompe l'esecuzione del processo nel caso in cui il codice di uscita specificato venga restituito.
   - **Esegui un comando dopo l'acquisizione della snapshot** - Immettere il comando di script da eseguire dopo l'acquisizione della snapshot.
   - **Esegui un comando al completamento del backup** - Immettere il comando di script da eseguire dopo il completamento del backup.
8. (Facoltativo) Fare clic sulla scheda Preferenze. Configurare i seguenti messaggi di avviso di posta elettronica, in base alle proprie esigenze:
   - Processi non eseguiti
   - Impossibile raggiungere il server vCenter/ESX (prima del backup)
   - Errore di licenza
   - Errore/arresto anomalo/annullamento del processo di backup, catalogo, ripristino o copia
   - Processo di backup, catalogo, ripristino o copia completato correttamente.
   - Spazio libero sulla destinazione inferiore a
   - Processo di unione interrotto, ignorato, con errori o arrestato in modo anomalo
   - Processo di unione eseguito correttamente
   - Ignorare/unire il processo in attesa nella coda dei processi

Se queste opzioni vengono abilitate, fare clic su Impostazioni di posta elettronica per configurare il server di posta elettronica. Fornire il tipo di servizio, il server di posta e la porta. Se è richiesta l'autenticazione, abilitare l'opzione di richiesta autenticazione, quindi fornire le credenziali.

- Specificare l'oggetto del messaggio di posta elettronica, ad esempio Avviso CA ARCserve Central Host-Based VM Backup.
- Specificare un valore Da, ad esempio, CA ARCserve Central Host-Based VM Backup.
- Specificare un indirizzo di posta elettronica per tutti i destinatari. Separare gli indirizzi mediante punto e virgola (;).

È possibile abilitare le impostazioni proxy specificando il nome del server proxy, la porta e le credenziali richieste.

Fare clic su OK.

9. Fare clic su Salva.

Modifica o copia di criteri di backup

CA ARCserve Central Host-Based VM Backup consente di modificare o copiare i criteri di backup di CA ARCserve D2D dopo la loro creazione.

Procedere come descritto di seguito:

1. Accedere all'applicazione.

   Fare clic su Criteri nella barra di navigazione per accedere alla schermata Criteri.

2. Dalla schermata Criteri, fare clic sulla casella di controllo corrispondente al criterio, quindi eseguire una delle seguenti operazioni:

   - Fare clic su Modifica della barra degli strumenti per modificare il criterio selezionato.
   - Fare clic su Copia della barra degli strumenti per copiare e creare un nuovo criterio dal criterio selezionato.

     Nota: la finestra di dialogo Copia criterio viene visualizzata quando viene eseguita la copia di un criterio. Specificare un nuovo nome per il criterio e fare clic su OK.

   Verrà visualizzata la finestra di dialogo Modifica criterio.

3. Se si desidera modificare il nome del criterio, specificare un nome nel campo Nome criterio.

4. Dalla scheda Impostazioni di backup, fare clic su Impostazioni di protezione e specificare le seguenti informazioni:

   - **Destinazione di backup** - Specificare una cartella condivisa remota per il salvataggio delle sessioni di backup.
   - **Proxy di backup del computer virtuale di CA ARCserve D2D** - Specificare il nome host o l'indirizzo IP del server su cui è stato installato CA ARCserve D2D. Se CA ARCserve D2D non è già stato installato, è possibile utilizzare CA ARCserve Central Protection Manager per la sua distribuzione. Fornire le credenziali appropriate per il server. Il valore predefinito per il numero di porta corrisponde a 8014. Se questo valore predefinito è stato modificato durante l'installazione di CA ARCserve D2D, specificare il numero di porta corretto.
   - **Impostazioni di memorizzazione** - È possibile impostare il criterio di memorizzazione in base al numero di punti di ripristino da memorizzare (unione delle sessioni) o al numero di set di ripristino da memorizzare (elimina i set di ripristino e disattiva i backup incrementali infiniti). L'opzione predefinita corrisponde a Mantieni i punti di ripristino. Per ulteriori informazioni, consultare la sezione Definizione delle impostazioni di protezione della Guida per l'utente di CA ARCserve Central Protection Manager.
   - **Compressione** - Selezionare un livello di compressione. Il valore predefinito è Standard. È possibile specificare i valori Nessuna compressione o Compressione massima.
   - **Crittografia** - Selezionare un livello di crittografia. Il valore predefinito corrisponde a Nessuna crittografia. Se si specifica un livello di crittografia, sarà necessario immettere una password di crittografia per il ripristino dei dati crittografati.
   - **Limite di velocità del backup** - Immettere la percentuale di scrittura dei backup su disco. Ridurre la percentuale per diminuire il carico di CPU o di rete. Tenere presente che l'operazione aumenta la durata del processo di backup. Questa opzione è disattivata per impostazione predefinita.

5. Fare clic su Pianificazione e completare le seguenti informazioni:

   - **Data e ora di inizio** - Specificare la data e l'ora di inizio desiderate per l'avvio dei processi di backup.
   - **Backup incrementale** - Definire una pianificazione ripetuta per i processi di backup incrementale. Il valore predefinito è impostato sulla ripetizione dei backup incrementali una volta al giorno.
   - **Backup completo** - Definire una pianificazione ripetuta per i processi di backup completo. Per impostazione predefinita, il valore è impostato per non essere mai ripetuto.
   - **Backup di verifica** - Definire una pianificazione ripetuta per i processi di backup di verifica. Per impostazione predefinita, il valore è impostato per non essere mai ripetuto.

6. Fare clic su Avanzate e completare le seguenti informazioni:

   - **Tronca registro** - Consente di abilitare le seguenti opzioni, nel caso in cui si desideri troncare i file di registro dell'applicazione.

     - **SQL Server** - Specificare una pianificazione di troncamento giornaliera, settimanale o mensile.

     - **Exchange Server** - Specificare una pianificazione di troncamento giornaliera, settimanale o mensile.

   - **Riserva spazio sulla destinazione** -Specifica la percentuale di spazio da riservare per l'esecuzione di un backup. Tale valore di spazio viene riservato immediatamente sulla destinazione prima che il backup avvii la scrittura dei dati, consentendo di aumentare la velocità di backup.

   - **Cataloghi** - Selezionare l'opzione di generazione del catalogo di file system per l'esecuzione di ricerche più veloci dopo il backup e ridurre i tempi di attesa durante la ricerca.

     Se questa opzione non è selezionata, è possibile eseguire immediatamente i ripristini dopo il backup senza dovere attendere il completamento del processo di catalogo. Per impostazione predefinita, l'opzione non è abilitata.

     Nota: se viene generato un catalogo di file system per ogni processo di backup, lo spazio necessario per l'archiviazione dei file di metadati e di catalogo sarà maggiore, così come l'utilizzo della CPU. Inoltre, se l'origine di backup contiene un numero elevato di file, il processo di generazione di un catalogo potrebbe richiedere tempi lunghi.

     Nota: se l'origine di backup selezionata è un volume NTFS deduplicato o un ReFS, non sarà possibile generare un catalogo e verrà visualizzato un messaggio di avviso che informa l'utente della condizione.

7. Fare clic su Impostazioni pre/post backup e specificare i comandi di pre o post backup desiderati. Se necessario, immettere le credenziali necessarie:
   - **Esegui un comando prima dell'avvio del backup** - Immettere il comando di script da eseguire prima dell'avvio del processo di backup.
   - **Sul codice di uscita** - Abilitare questa opzione se si desidera attivare il comando di script su un codice di uscita specifico.
   - **Esegui processo** - Se l'opzione è selezionata, il software procede con l'esecuzione del processo nel caso in cui il codice di uscita specificato venga restituito.
   - **Interrompi processo** - Se l'opzione è selezionata, il software interrompe l'esecuzione del processo nel caso in cui il codice di uscita specificato venga restituito.
   - **Esegui un comando dopo l'acquisizione della snapshot** - Immettere il comando di script da eseguire dopo l'acquisizione della snapshot.
   - **Esegui un comando al completamento del backup** - Immettere il comando di script da eseguire dopo il completamento del backup.
8. (Facoltativo) Fare clic sulla scheda Preferenze. Configurare gli avvisi di posta elettronica in base alle proprie esigenze. Se queste opzioni vengono abilitate, fare clic su Impostazioni di posta elettronica per configurare il server di posta elettronica.
9. Fare clic su Salva.

Il criterio viene modificato o copiato.

Assegnazione e annullamento assegnazione nodi da criteri di backup.

Per proteggere più computer virtuali, selezionare il criterio che si desidera utilizzare e assegnarlo a uno o più nodi.

Procedere come descritto di seguito:

1. Accedere all'applicazione.

   Fare clic su Criteri nella barra di navigazione per accedere alla schermata Criteri.
2. Dalla schermata Criteri, fare clic sulla scheda Assegnazione criterio.
3. Dall'elenco Criteri, selezionare il criterio da assegnare.

   Fare clic su Assegnazione e annullamento assegnazione per accedere alla finestra di dialogo Assegna/Annulla assegnazione criterio.

4. Specificare i campi seguenti nella finestra di dialogo Assegnazione/Annullamento assegnazione criterio:

   ■ **Gruppo:** selezionare il nome del gruppo contenente i nodi da assegnare.

   ■ **Filtro Nome nodo:** consente di filtrare i nodi disponibili in base a un criterio comune.

     Nota: il campo Nome nodo consente di filtrare i nodi mediante caratteri jolly.

     Ad esempio, Acc* consente di filtrare tutti i nodi il cui nome inizia per Acc. Per cancellare i risultati del filtro, fare clic su sul simbolo X del campo Filtro.

5. Effettuare una delle seguenti operazioni:

   ■ **Assegnazione di nodi ai criteri:** selezionare i nodi che si desidera aggiungere e fare clic sulla freccia destra singola.

     I nodi verranno spostati dall'elenco Nodi selezionati all'elenco Nodi selezionati.

     Nota: per selezionare e spostare tutti i nodi, fare clic sulla freccia destra doppia.

   ■ **Annullamento dell'assegnazione dei nodi dai criteri:** selezionare i nodi di cui si desidera annullare l'assegnazione, quindi fare clic sulla freccia sinistra singola.

     I nodi verranno spostati dall'elenco Nodi selezionati all'elenco Nodi disponibili.

     Nota: per selezionare e spostare tutti i nodi, fare clic sulla freccia sinistra doppia.

   Fare clic su OK.

6. Se necessario, immettere un nome utente e una password globali, quindi applicarli ai nodi selezionati.

   Fare clic su OK.

   I nodi selezionati vengono aggiunti all'elenco Assegnazione criterio e il loro stato di distribuzione viene definito su In attesa [Assegnato].

   Nota: è possibile visualizzare lo stato di distribuzione nella schermata Nodo.

7. Fare clic su Distribuisci ora per applicare immediatamente il criterio assegnato ai nodi specificati. Usare il pulsante Aggiorna per aggiornare lo stato.

Nella schermata Nodo, lo stato dei nodi specificati nell'elenco Assegnazione criterio mostra il criterio assegnato nella colonna Criterio. Fare clic sul nome del nodo, quindi selezionare Accesso a D2D per verificare lo stato dei processi di backup.

Visualizzazione di registri CA ARCserve Central Host-Based VM Backup

Il registro attività contiene informazioni complete su tutte le operazioni eseguite dall'applicazione. Il registro fornisce l'itinerario di controllo di ciascun processo eseguito (le attività più recenti vengono elencate in prima posizione) e può essere utile per la risoluzione di eventuali problemi.

Procedere come descritto di seguito:

1. Dalla pagina principale, fare clic su Visualizza registri della barra di navigazione.

   Verrà visualizzata la schermata Visualizza registri.

2. Utilizzare gli elenchi a discesa per specificare le informazioni di registro che si desidera visualizzare.

   - **Gravità** - Consente di specificare la gravità del registro che si desidera visualizzare. È possibile specificare le seguenti opzioni di gravità:

     - **Tutto** - Consente di visualizzare tutti i registri indipendentemente dalla gravità.
     - **Informazioni** - Consente di visualizzare unicamente i registri contenenti informazioni generali.
     - **Errori** - Consente di visualizzare unicamente i registri contenenti la descrizione degli errori gravi che si sono verificati.
     - **Avvisi** - Consente di visualizzare unicamente i registri contenenti la descrizione degli avvisi.
     - **Errori e avvisi** - Consente di visualizzare unicamente i registri di contenenti la descrizione degli errori gravi e di avviso che si sono verificati.

- **Modulo** - Consente di specificare il modulo di cui si desiderano visualizzare i registri. È possibile specificare le seguenti opzioni di modulo:
  - **Tutto** - Consente di visualizzare i registri relativi a tutti i componenti dell'applicazione.
  - **Comune** - Consente di visualizzare i registri relativi ai processi comuni.
  - **Importa nodi dal rilevamento** - Consente di visualizzare i registri relativi ai nodi importati unicamente mediante il rilevamento automatico.
  - **Importa nodi da hypervisor** - Consente di visualizzare i registri relativi ai nodi importati unicamente dall'hypervisor.
  - **Gestione criterio** - Consente di visualizzare unicamente i registri relativi alla gestione dei criteri.
  - **Aggiornamenti** - Consente di visualizzare unicamente i registri relativi all'aggiornamento dell'applicazione.
  - **Verifica preliminare** - Consente di visualizzare unicamente i registri che hanno eseguito lo stato di Verifica preliminare per ciascun nodo.
  - **Invia processi di backup del computer virtuale** - Consente di visualizzare unicamente i registri i cui nodi sono stati inviati per l'esecuzione di processi di backup del computer virtuale.
  - **Aggiorna nodi multipli** - Consente di visualizzare unicamente i registri relativi all'aggiornamento simultaneo di più nodi.
  - **Processo di unione CA ARCserve D2D** - Consente di visualizzare unicamente i registri relativi ai di processi di unione di CA ARCserve D2D.
- **Nome nodo** - Consente di visualizzare unicamente i registri relativi a un nodo specifico.

  Nota: questo campo supporta l'uso dei caratteri jolly '*' e '?'. Ad esempio, immettere 'lod*' per visualizzare tutti i registri attività per i computer il cui nome inizia per 'lod'.

Nota: è possibile applicare contemporaneamente le opzioni Gravità, Modulo e Nome nodo. Ad esempio, è possibile visualizzare Errori (Gravità) relativi agli Aggiornamenti (Modulo) per il Nodo X (Nome nodo).

La visualizzazione dei registri dipende dalle opzioni di visualizzazione specificate.

Nota: l'ora visualizzata nel registro dipende dal fuso orario del server di database dell'applicazione.

Visualizzare le informazioni sul registro attività per un nodo specifico

CA ARCserve Central Host-Based VM Backup consente di visualizzare le informazioni sul registro attività per uno specifico nodo di CA ARCserve D2D. Il Registro attività fornisce una traccia di controllo di ciascun processo eseguito (le attività più recenti vengono elencate in prima posizione) e può essere utile per la risoluzione di eventuali problemi.

Per visualizzare le informazioni sul registro attività per un nodo specifico

1. Aprire l'applicazione e fare clic su Nodo nella barra di navigazione.

   Verrà visualizzata la schermata Nodo.

2. Dall'elenco Gruppi, fare clic su Tutti i nodi oppure sul gruppo contenente il nodo CA ARCserve D2D a cui si desidera accedere.

   Nell'elenco dei nodi verranno visualizzati tutti i nodi associati al gruppo specificato.

3. Individuare e fare clic sul nodo a cui si desidera accedere, quindi su Accesso a D2D dal menu di scelta rapida.

   Verrà visualizzata la pagina principale del nodo di CA ARCserve D2D.

   Nota: se non viene aperta una nuova finestra, verificare che le opzioni del browser non blocchino la visualizzazione di tutti i popup o di quelli del sito Web corrente.

4. Fare clic su Visualizza registri nell'elenco Attività.

   Il Registro attività viene visualizzato come indicato di seguito:

   Il Registro attività fornisce le seguenti informazioni:

   - **Tipo -** Specifica la gravità dell'attività, che include informazioni, avvisi ed errori.
   - **ID processo -** Specifica il processo a cui si applica l'attività.
   - **Ora -** Specifica la data e l'ora a cui si applica l'attività.
   - **Messaggio -** Descrive l'attività.

5. Fare clic su OK per chiudere il Registro attività.

Visualizzazione dello stato di CA ARCserve Central Host-Based VM Backup in un rapporto

Se CA ARCserve Central Protection Manager e CA ARCserve Central Reporting sono stati installati, è possibile aggiungere il server proxy di backup dei computer virtuali basato su host a CA ARCserve Central Protection Manager, quindi generare il rapporto Stato di protezione della virtualizzazione per visualizzare lo stato del proxy di backup basato su host in uso.

Per ulteriori informazioni sul Rapporto Stato di protezione della virtualizzazione, consultare la Guida per l'utente di CA ARCserve Central Reporting.

Aggiungere collegamenti alla barra di spostamento

Per ogni applicazione CA ARCserve Central Applications è presente un collegamento Scheda Aggiungi nuovo sulla barra di navigazione. Questa funzionalità consente di aggiungere voci alla barra di navigazione per le ulteriori applicazioni Web che si desidera gestire. Tuttavia, per ciascuna applicazione installata, verrà aggiunto automaticamente un nuovo collegamento alla barra di navigazione. Ad esempio, se CA ARCserve Central Reporting e CA ARCserve Central Virtual Standby sono stati installati su un Computer A e CA ARCserve Central Reporting viene avviato, CA ARCserve Central Virtual Standby verrà aggiunto automaticamente alla barra di navigazione.

Nota: le applicazioni installate verranno rilevate soltanto se sono presenti altre istanze CA ARCserve Central Applications sullo stesso computer.

Procedere come descritto di seguito:

1. Dalla barra di navigazione dell'applicazione, fare clic sul collegamento Scheda Aggiungi nuovo.
2. Specificare il nome e l'URL per l'applicazione o il sito Web che si desidera aggiungere. Ad esempio, www.google.com.

   Facoltativamente, specificare il percorso di un'icona.
3. Fare clic su OK.

   La nuova scheda viene aggiunta nella parte inferiore della barra di navigazione.

Tenere presenti le seguenti considerazioni:

- Il collegamento al Supporto tecnico di CA viene aggiunto per impostazione predefinita.

Per rimuovere la nuova scheda, evidenziare la scheda e fare clic sul collegamento Rimuovi.

Considerazioni sulla protezione dei mapping di periferiche raw

Tenere presente il seguente comportamento per la protezione di mapping di periferiche raw (RDM):

- L'applicazione non supporta la protezione di mapping di periferiche raw in modalità di compatibilità fisica (i dischi di questo tipo sono periferiche fisiche). L'applicazione omette i mapping di periferiche raw in modalità di compatibilità fisica dall'origine di backup durante il processo di backup. Per risolvere il problema, si consiglia di installare CA ARCserve D2D sul sistema operativo guest e di usare la stessa procedura di backup dei dischi fisici.

- L'applicazione supporta la protezione dei mapping di periferiche raw in modalità di compatibilità virtuale. Tenere tuttavia presenti le seguenti considerazioni:
  - Per quanto riguarda i backup completi, l'applicazione consente di eseguire il backup di dischi di mapping di periferiche raw in modalità di compatibilità virtuale. Tuttavia, se non si utilizza la compressione di dati, i set di dati di backup possono avere la stessa dimensione del disco di origine.
  - CA ARCserve Central Host-Based VM Backup esegue il ripristino dei dischi RDM in modalità di compatibilità virtuale come dischi virtuali normali. Una volta completato il processo di recupero, il disco non sarà più configurato come disco virtuale RDM o non ne seguirà più il comportamento.
  - Un approccio alternativo per eseguire il backup di periferiche raw in modalità di compatibilità virtuale consiste nell'installare CA ARCserve D2D nel sistema operativo guest ed eseguire il backup di periferiche raw nella stessa modalità utilizzata per il backup di computer fisici.

Modifica del protocollo di comunicazione del server

Per impostazione predefinita, CA ARCserve Central Applications utilizza il protocollo HTTP (Hypertext Transfer Protocol) per la comunicazione tra i componenti. Se si desidera utilizzare un livello di protezione superiore per la comunicazione delle password tra i componenti, è possibile utilizzare il protocollo HTTPS (Hypertext Transfer Protocol Secure). Se non si desidera utilizzare tale livello di protezione aggiuntivo, è possibile modificare il protocollo utilizzato selezionando HTTP.

Procedere come descritto di seguito:

1. Accedere al computer di installazione dell'applicazione utilizzando un account amministrativo o un account con privilegi di amministratore.

   Nota: se l'accesso non viene eseguito con un account amministrativo o un con privilegi di amministratore, sarà necessario configurare la riga di comando per l'esecuzione con privilegi di amministratore.

2. Aprire la riga di comando di Windows.

3. Eseguire una delle seguenti operazioni:

   - **Per modificare il protocollo da HTTP a HTTPS:**

     Avviare l'utilità "changeToHttps.bat" dal percorso predefinito riportato di seguito (la posizione della cartella BIN può variare in base al percorso di installazione dell'applicazione):

     ```
     C:\Programmi\CA\ARCserve Central Applications\BIN
     ```

     Una volta apportate le modifiche al protocollo, verrà visualizzato il messaggio seguente:

     ```
     Il protocollo di comunicazione è stato convertito in HTTPS.
     ```

   - **Per modificare il protocollo da HTTPS a HTTP:**

     Avviare l'utilità "changeToHttp.bat" dal percorso predefinito riportato di seguito (la posizione della cartella BIN può variare in base al percorso di installazione dell'applicazione):

     ```
     C:\Programmi\CA\ARCserve Central Applications\BIN
     ```

     Una volta apportate le modifiche al protocollo, verrà visualizzato il messaggio seguente:

     ```
     Il protocollo di comunicazione è stato convertito in HTTP.
     ```

4. Riavviare il browser e connettersi nuovamente a CA ARCserve Central Applications.

   Nota: in caso di modifica del protocollo in HTTPS, verrà visualizzato un avviso nel browser Web. Questo comportamento è causato da un certificato di protezione autofirmato che richiede all'utente di ignorare l'avviso e continuare oppure di aggiungere il certificato al browser per evitarne la visualizzazione.

Definizione di una modalità di trasporto per i backup

È possibile definire una modalità di trasporto specifica (trasferimento dei dati) da utilizzare per i processi di backup di D2D che vengono eseguiti mediante CA ARCserve Central Host-Based VM Backup. Per impostazione predefinita, i processi di backup del computer virtuale basati su host utilizzano una modalità che consente a CA ARCserve Central Host-Based VM Backup di ottimizzare le prestazioni (aumento della velocità) delle operazioni di backup. Tuttavia, se si desidera specificare una determinata modalità di trasporto per le operazioni di backup, è possibile configurare la chiave di registro descritta nella presente sezione.

CA ARCserve Host-Based VM Backup è in grado di eseguire i backup mediante le seguenti modalità di trasporto:

- Modalità di trasporto HOTADD (a pagina 203)
- Modalità di trasporto NBD (a pagina 203)
- Modalità di trasporto NBDSSL (a pagina 203)
- Modalità di trasporto SAN (a pagina 203)

Tenere presenti le seguenti considerazioni:

- Si tratta di un'attività di configurazione facoltativa. Per impostazione predefinita, CA ARCserve Central Host-Based VM Backup esegue i backup mediante la modalità di trasporto in grado di ottimizzare la prestazioni dell'operazione di backup.
- Quando si configura questa chiave di registro per utilizzare una modalità di trasporto specifica e la modalità non è disponibile, CA ARCserve Central Host-Based VM Backup utilizza una modalità di trasporto predefinita disponibile per il backup.

Procedere come descritto di seguito:

1. Accedere al sistema proxy di backup CA ARCserve D2D per i computer virtuali.

   Aprire l'editor del Registro di sistema di Windows e cercare la seguente chiave:

   ```
   [HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA ARCSERVE
   D2D\AFBackupDll\{VM-InstanceUUID}].
   ```

2. Fare clic con il pulsante destro del mouse su VM-InstanceUUID, scegliere Nuovo e quindi Valore stringa dal menu di scelta rapida.

   Nominare il nuovo valore della stringa come segue:

   ```
   EnforceTransport
   ```

3. Fare clic con il tasto destro del mouse sull'opzione EnforceTransport, quindi su Modifica del menu di scelta rapida per aprire la finestra di dialogo di modifica della stringa.

4. Nel campo Dati del valore, specificare la modalità di trasporto che si desidera utilizzare durante il processo di backup. Specificare uno dei seguenti valori:

   hotadd

   Modalità di trasporto HOTADD (a pagina 203)

   nbd

   Modalità di trasporto NBD (a pagina 203)

   nbdssl

   Modalità di trasporto NBDSSL (a pagina 203)

   san

   Modalità di trasporto SAN (a pagina 203)

5. Fare clic su OK per applicare il valore e chiudere la finestra di dialogo di modifica della stringa.

La modalità di trasporto viene definita e viene utilizzata con l'esecuzione successiva del processo.

Capitolo 4: Ripristino e recupero di computer virtuali

Le opzioni di ripristino e recupero disponibili dipendono dalla modalità di esecuzione del backup del sistema. Ad esempio, non è possibile utilizzare le sessioni di backup create con CA ARCserve Central Host-Based VM Backup per eseguire operazioni di ripristino granulare su Microsoft Exchange o a livello di applicazione, ma è possibile eseguire questa operazione con sessioni create con CA ARCserve Central Protection Manager o CA ARCserve D2D. Alcune opzioni di ripristino di CA ARCserve D2D potrebbero non essere disponibili con questa applicazione. Ad esempio, l'opzione Ripristina in posizione originale non può essere utilizzata nei backup dell'applicazione in quanto la posizione del server proxy non coincide con la posizione del computer virtuale di origine di backup.

Per ulteriori informazioni sull'uso dei Metodi di ripristino (a pagina 110), consultare la sezione Considerazioni sul ripristino. (a pagina 96)

Questa sezione contiene i seguenti argomenti:

Metodi di ripristino

Il metodo di ripristino dipende dalla modalità utilizzata per la creazione della sessione di backup. Ad esempio, alcuni metodi di ripristino sono disponibili solo se eseguiti da una versione di CA ARCserve D2D installata in locale. Altri metodi richiedono l'attivazione del computer virtuale al momento del backup.

Sfoglia punti di ripristino **(a pagina 97)**

Consente di individuare i punti di ripristino disponibili (backup completati con successo) da una visualizzazione calendario. Utilizzare questo metodo per il ripristino di file e cartelle, oppure per eseguire il processo di ripristino a livello di applicazione.

Tale metodo può essere utilizzato per il ripristino dei backup creati con CA ARCserve D2D, CA ARCserve Central Host-Based VM Backup, o CA ARCserve Central Protection Manager.

Trova file/cartelle da ripristinare **(a pagina 101)**

Consente di individuare file o cartelle specifiche per il ripristino.

Questo metodo può essere utilizzato per il ripristino dei backup creati con CA ARCserve D2D. Inoltre è possibile utilizzare questo metodo per ripristinare i backup creati con CA ARCserve Central Host-Based VM Backup e CA ARCserve Central Protection Manager se il computer virtuale viene attivato al momento del backup.

Recupera computer virtuale **(a pagina 104)**

Consente di sfogliare i punti di ripristino del computer virtuale (backup completati con successo) da una visualizzazione calendario e specificare il computer virtuale da recuperare.

Questo metodo, disponibile per il ripristino dei backup creati con CA ARCserve Central Host-Based VM Backup, esegue il provisioning del computer virtuale e il ripristino del sistema operativo, delle applicazioni e dei dati dal punto di ripristino specificato.

Ripristino dell'applicazione **(a pagina 110)**

Per il ripristino completo di un server Microsoft Exchange o SQL senza dover eseguirne la rigenerazione, fare clic sul metodo Sfoglia punti di ripristino da una versione CA ARCserve D2D installata in locale.

Ripristino Bare Metal (a pagina 161)

Il processo di ripristino bare metal (BMR) consiste nel ripristino di un intero computer, incluso il sistema operativo, le applicazioni software, le impostazioni e i dati. Per eseguire il ripristino bare metal è necessario disporre di un'immagine o del kit di avvio di Windows e di almeno un backup completo. Questo metodo può essere utilizzato per il ripristino dei backup creati con CA ARCserve D2D, CA ARCserve Central Host-Based VM Backup, CA ARCserve Central Virtual Standby e CA ARCserve Central Protection Manager. Tuttavia, in caso di disattivazione del computer virtuale durante il backup non sarà possibile eseguire il ripristino bare metal.

Ripristino da punti di ripristino

Il metodo Sfoglia punti di ripristino consente di individuare i backup completati correttamente (punti di ripristino denominati) da una visualizzazione calendario. È possibile individuare e selezionare i contenuti di backup (applicazioni incluse) da ripristinare. La procedura utilizzata per il ripristino mediante il metodo Sfoglia punti di ripristino è identica a quella di CA ARCserve D2D, con una sola eccezione. Per ripristinare i punti di ripristino del computer virtuale, non è possibile utilizzare l'opzione di ripristino in posizione originale.

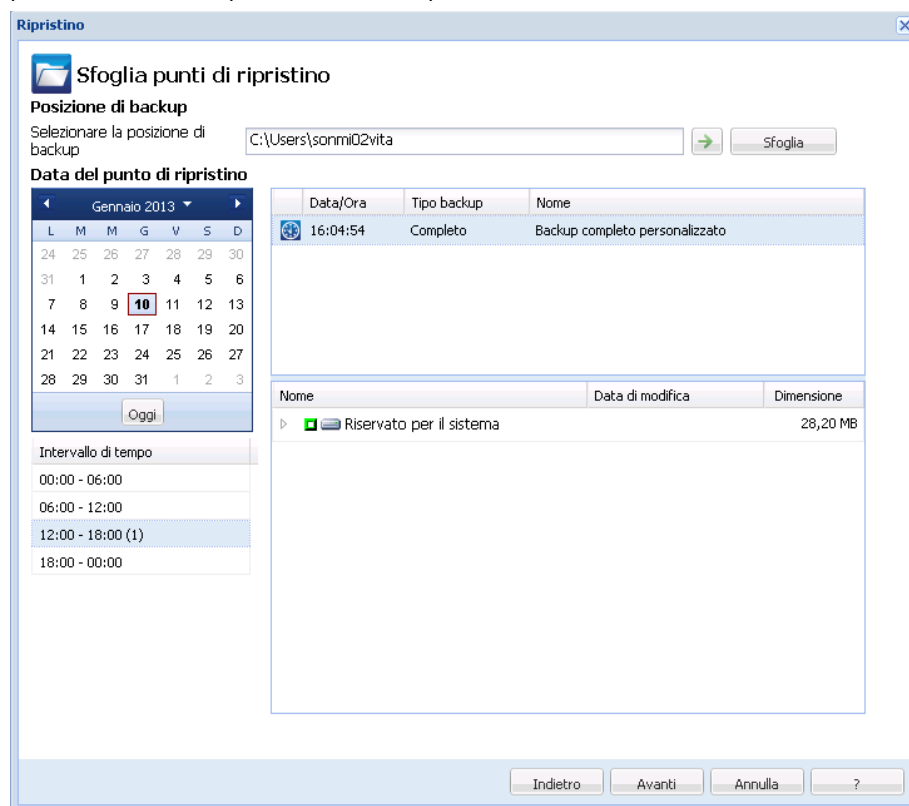
Procedere come descritto di seguito:

1. Accedere all'applicazione e fare clic su Nodo sulla barra di navigazione.

   Dalla schermata Nodo, espandere il gruppo contenente il nodo da ripristinare.

   Fare clic sulla casella di controllo accanto al nodo da ripristinare e selezionare Ripristina dalla barra degli strumenti.

2. Nella finestra di dialogo Ripristino, fare clic su Sfoglia punti di ripristino.

   In base al nodo selezionato, viene visualizzata la posizione di backup corrispondente nella finestra di dialogo Ripristina. Se lo si desidera, immettere le credenziali utente per selezionare una posizione di backup diversa.

3. Fare clic sulla data del punto di ripristino e selezionare un orario. Selezionare il contenuto da ripristinare. È possibile selezionare un intero volume oppure un file, una cartella, un database, o un'applicazione. Gli elementi selezionati per il ripristino sono contrassegnati mediante una casella piena di colore verde. Al termine dell'operazione, fare clic su Avanti.

4. Specificare la destinazione di ripristino nella finestra di dialogo Opzioni di ripristino.
   - **Ripristina in posizione originale (disabilitato)** - Per le sessioni CA ARCserve Central Host-Based VM Backup, non è possibile effettuare ripristini in posizione originale. Per ripristinare file o cartelle in posizione originale nel sistema operativo guest di un computer virtuale, è necessario installare CA ARCserve D2D sul sistema operativo guest del computer virtuale oppure effettuare il ripristino su una cartella condivisa di rete del computer virtuale.
   - **Ripristina su** - Specificare la destinazione di ripristino.
   - **Sovrascrivi i file esistenti** - Sostituisce i file della destinazione.
   - **Sostituisci file attivi** - Sostituisce i file in uso o i file aperti al momento del riavvio.
   - **Rinomina file** - Crea un nuovo file se il nome file è già esistente. Questa opzione consente di copiare i file di origine nella destinazione con lo stesso nome file ma con un'estensione diversa. I dati vengono quindi ripristinati nel file con la nuova estensione.
   - **Ignora file esistenti** - Ignora e non sostituisce i file esistenti contenuti nella destinazione. Si tratta dell'impostazione predefinita.
   - **Crea directory principale** - Ricrea la stessa struttura di directory principale sulla destinazione rilevata nell'immagine di backup.
5. Fare clic su Avanti. Nella schermata Riepilogo di ripristino, verificare che le opzioni siano corrette. In caso contrario, fare clic su Indietro. Se le impostazioni sono corrette, fare clic su Fine per avviare il processo di ripristino.

Ripristino mediante il montaggio di un punto di ripristino

Il metodo di ripristino Monta punto di ripristino consente di eseguire montaggio di un punto di ripristino sul sistema proxy di backup. Per montare un punto di ripristino, accedere all'interfaccia utente di CA ARCserve D2D.

Procedere come descritto di seguito:

1. Eseguire l'accesso a CA ARCserve Central Host-Based VM Backup e fare clic su Nodo nella barra di navigazione.
2. Dalla schermata Nodo, espandere il gruppo contenente il nodo da ripristinare.

   Fare clic sulla casella di controllo accanto al nodo da ripristinare e selezionare Ripristina dalla barra degli strumenti.

   Viene aperta la versione CA ARCserve Central Host-Based VM Backup di CA ARCserve D2D.

   Nota: verificare che le opzioni del browser cosentino la visualizzazione di tutti i popup o dei popup del sito Web corrente, per poter aprire una nuova finestra del browser.

Per ulteriori informazioni sulla finestra di dialogo Monta punto di ripristino, fare clic sul collegamento alla guida in linea della finestra dalla pagina principale di CA ARCserve D2D.

Ripristino di dati mediante l'opzione Trova file/cartelle da ripristinare

Al completamento di ogni backup, tutti i file o le cartelle di cui è stato eseguito il backup vengono incluse nell'immagine snapshot del backup. Questo metodo di ripristino consente di specificare esattamente i file o le cartelle da ripristinare.

Procedere come descritto di seguito:

1. Accedere all'applicazione e fare clic su Nodo sulla barra di navigazione.

   Dalla schermata Nodo, espandere il gruppo contenente il nodo da ripristinare.

   Fare clic sulla casella di controllo accanto al nodo da ripristinare e selezionare Ripristina dalla barra degli strumenti.
2. Dalla finestra di dialogo Ripristino, fare clic su Trova file/cartelle da ripristinare.
3. Nella finestra di dialogo Trova file/cartelle da ripristinare, specificare o individuare la posizione di backup. In caso di ripristino da una sessione di CA ARCserve Central Host-Based VM Backup, non sarà possibile specificare la posizione di backup. È possibile eseguire il ripristino di copia file solo in caso di ripristino dalle sessioni di backup CA ARCserve Central Protection Manager o CA ARCserve D2D.

4. Specificare il nome del file o della cartella da ripristinare.

   Nota: il campo Nome file supporta la ricerca per nome completo e con caratteri jolly. Se non si conosce il nome file completo, è possibile semplificare i risultati della ricerca immettendo i caratteri jolly "*" e "?" nel campo Nome file.

   I caratteri jolly supportati per il nome dei file o delle cartelle sono i seguenti:

   - "*" - Utilizzare l'asterisco per sostituire zero o più caratteri in un nome di file o directory.
   - "?" - Utilizzare il punto interrogativo per sostituire un singolo carattere nel nome di un file o di una directory.

   Ad esempio, specificando *.txt, la ricerca restituirà tutti i file con estensione .txt.

5. (Facoltativo) Specificare il nome di un percorso per filtrare ulteriormente la ricerca, indicando se includere o meno sottodirectory, file e cartelle.

6. Fare clic su Trova per dare inizio alla ricerca.

   Verranno visualizzati i risultati di ricerca. Se vengono rilevate più occorrenze (punti di ripristino) dello stesso file di ricerca, verranno elencate tutte le occorrenze in ordine cronologico (dalla più recente alla meno recente).

7. Selezionare la versione di cui si desidera eseguire il ripristino dall'elenco e fare clic su Avanti.

   Verrà visualizzata la finestra di dialogo Opzioni di ripristino. Il ripristino potrà essere eseguito solo in una posizione alternativa. Specificare o individuare la posizione di archiviazione dell'immagine di backup. Fare clic sulla freccia verde per verificare la connessione. Se necessario, immettere le credenziali utente.

8. Selezionare le opzioni di risoluzione del conflitto:

   Sovrascrivi i file esistenti

   Sovrascrive (sostituisce) i file esistenti nella destinazione di ripristino. Tutti gli oggetti verranno ripristinati dai file di backup, indipendentemente dalla loro presenza sul computer.

   Sostituisci file attivi

   Consente di sostituire i file attivi dopo il riavvio. Se durante il tentativo di ripristino il software rileva che il file esistente è momentaneamente in uso, tale file non verrà sostituito immediatamente. Per evitare l'insorgere di problemi, i file attivi verranno sostituiti al riavvio successivo del computer. (Il ripristino verrà eseguito immediatamente, ma la sostituzione dei file attivi verrà eseguita con il riavvio successivo).

   Nota: se questa opzione non viene selezionata, tutti i file attivi verranno ignorati dal processo di ripristino.

   Rinomina file

   Se il nome file esiste già, consente di creare un nuovo file. Consente di copiare il file di origine nella destinazione con lo stesso nome file ma con un'estensione diversa. I dati verranno quindi ripristinati nel nuovo file.

   Ignora file esistenti

   Ignora e non sovrascrive (sostituisce) i file esistenti contenuti nella destinazione di ripristino. Verrà eseguito il ripristino dai file di backup solo degli oggetti non presenti sul computer.

   Questa opzione è selezionata per impostazione predefinita.

9. (Facoltativo) Selezionare Crea directory principale dalla struttura directory.

   Questa opzione consente di ricreare la stessa struttura della directory principale nel percorso di destinazione di ripristino.

   Nota: se questa opzione non viene selezionata, il file o la cartella da ripristinare verranno ripristinati direttamente nella cartella di destinazione.

10. Immettere la password di crittografia del backup per ripristinare i dati codificati quindi fare clic su Avanti.

    Verrà visualizzata la finestra di dialogo Riepilogo di ripristino.

11. Verificare che le opzioni di ripristino e le impostazioni siano corrette.

    - Se le informazioni di riepilogo non sono corrette, fare clic su Indietro e accedere alla finestra di dialogo corrispondente per modificare le impostazioni non corrette.
    - Se le informazioni di riepilogo sono corrette, fare clic su Fine per avviare il processo di ripristino.

Recupero di un intero computer virtuale

È possibile eseguire il recupero di un intero computer virtuale da una sessione di CA ARCserve Central Host-Based VM Backup.

Questo metodo di backup è simile al ripristino bare metal e consente di eseguire il recupero del sistema operativo guest Windows, delle applicazioni e dei dati.

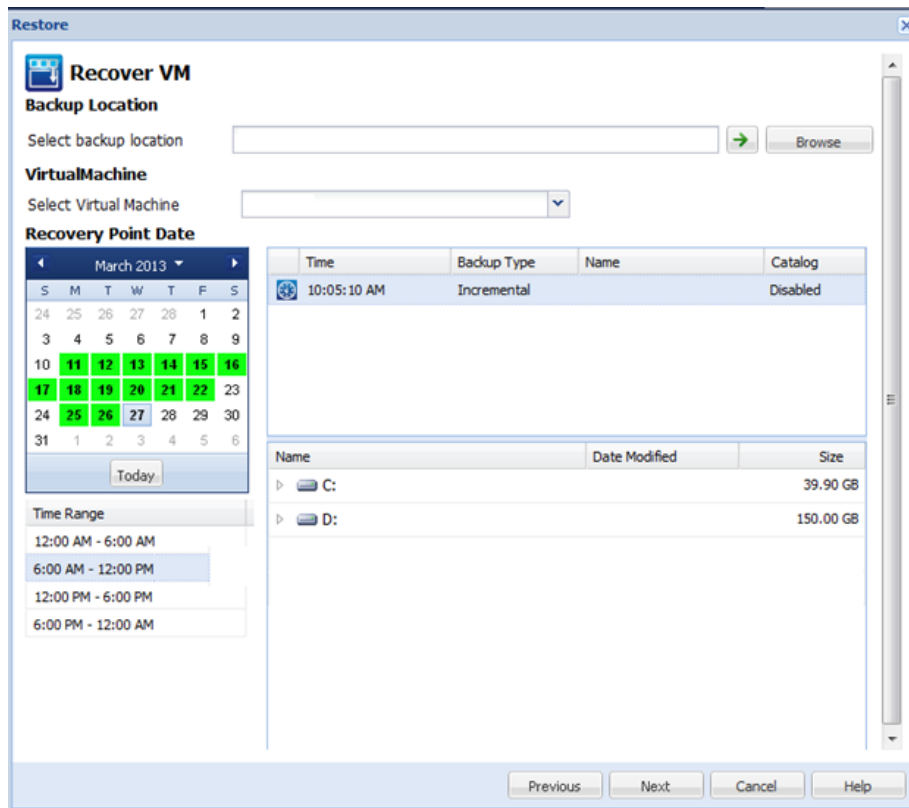
Procedere come descritto di seguito:

1. Accedere all'applicazione e fare clic su Nodo sulla barra di navigazione.

   Dalla schermata Nodo, espandere il gruppo contenente il nodo da ripristinare.

   Fare clic sulla casella di controllo accanto al nodo da ripristinare e selezionare Ripristina dalla barra degli strumenti. L'applicazione effettua l'accesso dell'utente a CA ARCserve D2D.

2. Dalla finestra di dialogo Ripristino, fare clic su Recupera computer virtuale.

3. Verrà visualizzata la finestra di dialogo di ripristino. I campi Posizione di backup e Computer virtuale vengono compilati con in dati del computer virtuale selezionati dalla schermata Nodo. Se lo si desidera, è possibile modificare i valori.

Specificare l'origine di archiviazione delle sessioni di backup del computer virtuale. Se richiesto, immettere le credenziali utente.

Il menu a discesa del campo Posizione di backup elenca i computer virtuali della posizione.

4. Nel calendario, fare clic sulla data corrispondente all'immagine del computer virtuale che si desidera recuperare. Dall'elenco Intervallo di tempo, fare clic sull'immagine di backup da recuperare. Il contenuto corrispondente alla selezione viene visualizzato come riferimento. Non è possibile selezionare volumi, cartelle, o file individuali. Verrà eseguito il ripristino dell'intero computer virtuale.

5. Fare clic su Avanti. Nella finestra di dialogo Opzioni di ripristino, specificare la destinazione di ripristino.

   Ripristina in posizione originale

   Esegue il ripristino sul computer virtuale nel percorso in cui è stata acquisita l'immagine di backup. Questa opzione è selezionata per impostazione predefinita.

   Per ulteriori informazioni, consultare la sezione Ripristino del computer virtuale in posizione originale (a pagina 106).

   Ripristino in una posizione alternativa

   Esegue il ripristino sul computer virtuale in un percorso diverso da quello in cui è stata acquisita l'immagine di backup.

   Per ulteriori informazioni, consultare la sezione Ripristino del computer virtuale in una posizione alternativa (a pagina 107).

6. Specificare le opzioni di risoluzione del conflitto e di post-recupero. Per impostazione predefinita, tali opzioni sono deselezionate.

   - Sovrascrivi il computer virtuale esistente - Sostituisce qualsiasi immagine di computer virtuale esistente sul server vCenter/ESX.
   - Attiva computer virtuale - Avvia il computer virtuale al completamento del processo di ripristino.

7. Fare clic su Avanti. Se richiesto, immettere le credenziali del server Vcenter/ESX per l'origine di backup, e fare clic su OK.

8. Nella schermata Riepilogo di ripristino, verificare che tutte le opzioni siano corrette. In caso contrario, fare clic su Indietro. Se le impostazioni sono corrette, fare clic su Fine per avviare il processo di recupero.

Ripristino di computer virtuali nella posizione originale

Durante il processo di configurazione del ripristino del computer virtuale, è necessario selezionare la posizione in cui di desidera ripristinare il computer virtuale. Le opzioni disponibili sono Ripristina in posizione originale e Ripristina in posizione alternativa.

Se si seleziona per il ripristino del computer virtuale in posizione originale, attenersi ai seguenti passaggi:

Procedere come descritto di seguito:

1. Dalla finestra di dialogo Opzioni di ripristino, dopo aver specificato le opzioni Risolvi conflitti e Post-recupero, selezionare l'opzione Ripristina in posizione originale, quindi fare clic su Avanti.

   Nota: per ulteriori informazioni sulle opzioni Risolvi conflitti e Post-recupero, consultare la sezione Ripristino dei dati da computer virtuali.

   Verrà visualizzata la finestra di dialogo di impostazione delle credenziali per il server Vcenter/ESX di origine.

2. Specificare le credenziali di accesso al computer virtuale.

   - **Server vCenter/ESX** - Specifica il nome host o l'indirizzo IP del sistema server vCenter o ESX di destinazione.
   - **Nome del computer virtuale** - Specifica il nome host del computer virtuale di cui si sta eseguendo il ripristino.
   - **Protocollo -** Specifica il protocollo da utilizzare per la comunicazione con il server di destinazione. Le opzioni disponibili sono HTTP e HTTPS.
   - **Numero di porta -** Specifica la porta da utilizzare per il trasferimento dei dati tra il server di origine e il server di destinazione. Per impostazione predefinita, il numero di porta è 443.
   - **Nome utente** - Consente di specificare il nome dell'utente che dispone dell'autorizzazione per l'accesso al computer virtuale da ripristinare.
   - **Password** - Specifica la password corrispondente al nome utente richiesto per l'accesso al computer virtuale di cui si sta eseguendo il ripristino.

3. Dopo aver specificato le credenziali, fare clic su OK.

   Verrà visualizzata la finestra di dialogo Riepilogo di ripristino.

4. Verificare che le opzioni di ripristino e le impostazioni siano corrette.

   - Se le informazioni di riepilogo non sono corrette, fare clic su Indietro e accedere alla finestra di dialogo corrispondente per modificare le impostazioni non corrette.
   - Se le informazioni di riepilogo sono corrette, fare clic su Fine per avviare il processo di ripristino.

Ripristino di computer virtuali in posizioni alternative

Durante il processo di configurazione del ripristino del computer virtuale, è necessario selezionare la posizione in cui di desidera ripristinare il computer virtuale. Le opzioni disponibili sono Ripristina in posizione originale e Ripristina in posizione alternativa.

Se si desidera ripristinare il computer virtuale in una posizione alternativa, attendersi alla seguente procedura:

Procedere come descritto di seguito:

1. Dalla finestra di dialogo Opzioni di ripristino, dopo aver specificato le opzioni Risolvi conflitti e Post-recupero, selezionare l'opzione Ripristina in posizione alternativa.

   Nota:per ulteriori informazioni sulle opzioni Risolvi conflitti e Post-recupero, consultare la sezione Recupero dei dati su computer virtuali.

   La finestra di dialogo Opzioni di ripristino verrà espansa per visualizzare ulteriori opzioni di ripristino in posizione alternativa.

2. Specificare le informazioni del server vCenter/ESX.

   - **Server vCenter/ESX** - Specifica il nome host o l'indirizzo IP del sistema server vCenter o ESX di destinazione.
   - **Nome utente** - Consente di specificare il nome dell'utente che dispone dei privilegi di accesso per il computer virtuale da ripristinare.
   - **Password** - Specifica la password corrispondente al nome utente richiesto per l'accesso al computer virtuale di cui si sta eseguendo il ripristino.
   - **Protocollo -** Specifica il protocollo da utilizzare per la comunicazione con il server di destinazione. Le opzioni disponibili sono HTTP e HTTPS.
   - **Numero di porta -** Specifica la porta da utilizzare per il trasferimento dei dati tra il server di origine e il server di destinazione. Per impostazione predefinita, il numero di porta è 44.

3. Dopo aver specificato le informazioni del server vCenter/ESX, fare clic sul pulsante Connetti a questo server vCenter/ESX.

   Se le informazioni per l'accesso al server alternativo sono corrette, verrà abilitato il campo Ulteriori informazioni.

4. Immettere le informazioni richieste.

   - **Nome del computer virtuale** - Specifica il nome host del computer virtuale di cui si sta eseguendo il ripristino.
   - **Server ESX** - Specifica il server ESX di destinazione. Il menu a discesa contiene un elenco di tutti i server ESX associati al computer virtuale specificato.
   - **Pool di risorse** - Specifica il pool di risorse o il pool vApp da utilizzare per il recupero del computer virtuale. Fare clic sul pulsante che consente di sfogliare il pool di risorse per visualizzare la finestra di dialogo Selezionare un pool di risorse. Questa finestra di dialogo contiene un elenco di tutti i pool di risorse e i pool vApp disponibili per il server ESX di destinazione. Selezionare il pool da utilizzare per il ripristino del computer virtuale. È possibile lasciare vuoto il campo se non si desidera assegnare un pool di risorse o un pool vApp per il ripristino di questo computer virtuale.

     Nota: un pool di risorse è una raccolta configurata di CPU e di risorse di memoria. Un pool vApp è una raccolta di uno o più computer virtuali che può essere gestita come un singolo oggetto.

   - **Archivio dati del computer virtuale** - Specifica l'archivio dati del computer virtuale per il ripristino del computer virtuale o qualsiasi disco virtuale del computer virtuale.

     Un computer virtuale può avere più dischi virtuali ed è possibile specificare un archivio dati distinto per ciascuno di essi.

     Esempio:

     - Disk0 può essere ripristinato su Datastore1.
     - Disk1 può essere ripristinato su Datastore1.
     - Disk2 può essere ripristinato su Datastore2.

     Importante. Per l'archivio dati del computer virtuale, il campo viene compilato soltanto se l'utente dispone delle autorizzazioni di amministratore per il sistema VMware. Se l'utente non dispone delle autorizzazioni di amministratore appropriate, CA ARCserve Central Host-Based VM Backup non eseguirà il processo di ripristino una volta stabilita la connessione al server vCenter/ESX.

5. Dopo aver immesso tutte le informazioni necessarie, fare clic su Avanti.

   Verrà visualizzata la finestra di dialogo Riepilogo di ripristino.

6. Verificare che le opzioni di ripristino e le impostazioni siano corrette.

   - Se le informazioni di riepilogo non sono corrette, fare clic su Indietro e accedere alla finestra di dialogo corrispondente per modificare le impostazioni non corrette.
   - Se le informazioni di riepilogo sono corrette, fare clic su Fine per avviare il processo di ripristino.

Considerazioni sul ripristino

Utilizzare la tabella seguente per determinare quale metodo di ripristino utilizzare nelle condizioni elencate.

Metodo di ripristino:	Attività:	Considerazioni:
Sfoglia punti di ripristino (Utilizzare questo metodo per il ripristino a livello di applicazione.) Trova file/cartelle da ripristinare	Ripristinare file, cartelle, database o applicazioni danneggiate.	■ **CA ARCserve Central Host-Based VM Backup**: per il ripristino di file o cartelle è necessario attivare il computer virtuale al momento del backup. L'opzione Ripristina in posizione originale non è disponibile. Eseguire il mapping di un'unità di rete sul percorso originale oppure accedere all'unità in modalità condivisa ed eseguire il ripristino sulla posizione condivisa o di mapping. Installare CA ARCserve D2D sul sistema operativo guest di un nuovo computer virtuale e ripristinare un database di applicazione. Per ulteriori informazioni, consultare la sezione Ripristini a livello di applicazione. ■ **CA ARCserve D2D o CA ARCserve Central Protection Manager**: consultare la Guida per l'utente dell'applicazione.
Recupera computer virtuale	Eseguire il provisioning di un nuovo computer virtuale, ripristinare il sistema operativo, le applicazioni e i dati.	■ **CA ARCserve Central Host-Based VM Backup**: consigliato ■ **CA ARCserve D2D o CA ARCserve Central Protection Manager**: non supportato

È inoltre possibile eseguire il recupero mediante il ripristino bare metal e il processo di ripristino a livello di applicazione. Per ulteriori informazioni, consultare la sezione Metodi di ripristino (a pagina 96).

Ripristini a livello di applicazione

CA ARCserve Central Applications consente di proteggere e recuperare i dati nonché di recuperare le applicazioni che utilizzano tali dati. I ripristini a livello di applicazione utilizzano il metodo di ripristino Sfoglia punti di ripristino. Durante il processo di ripristino a livello di applicazione, è possibile eseguire il recupero dei server Microsoft Exchange o SQL senza dover eseguire un ripristino di emergenza completo.

Prima di avviare il processo di ripristino a livello di applicazione potrebbe essere necessario effettuare le seguenti operazioni:

- Fornire un nuovo computer virtuale con sistema operativo guest Windows.
- Installare CA ARCserve D2D sul sistema operativo guest.
- Per le operazioni di ripristino dell'applicazione Exchange Server:
  - Verificare che l'account disponga dei privilegi di Amministratore completo di Exchange per Exchange Server 2003, oppure di Amministratore dell'organizzazione di Exchange o Amministratore di del server per Exchange Server 2007/2010/2013.
  - Quando viene eseguito il ripristino dei database Exchange Server 2007 su gruppi di archiviazione di recupero, è necessario creare i gruppi di archiviazione di recupero sul server protetto. Allo stesso modo, quando viene eseguito il ripristino dei database Exchange Server 2010 o 2013 sui database di recupero, è necessario creare i database di recupero sul server protetto.
  - Consultare la procedura completa per l'esecuzione del ripristino fornita nella Guida per l'utente di CA ARCserve D2D.

Ripristino dei dati del server Exchange

È possibile eseguire ripristini a livello di applicazione dei dati Microsoft Exchange Server con:

- Exchange Server 2003 - Ambiente con server singolo. L'ambiente cluster non è supportato.
- Exchange Server 2007 - Ambiente con server singolo, replica continua locale (LCR) e replica continua cluster (CCR). In ambiente Exchange 2007 CCR, è necessario installare localmente CA ARCserve D2D sia sul nodo attivo che sul nodo passivo. È possibile eseguire le operazioni di backup dal nodo attivo e dal nodo passivo, mentre le operazioni di ripristino possono essere eseguite solamente sul nodo attivo. Single Copy Cluster (SCC) non è supportato.
- Exchange Server 2010 - Ambiente con server singolo e per gruppo di disponibilità del database (DAG). Per gli ambienti DAG, verificare che CA ARCserve D2D sia stato installato su tutti i server del gruppo di disponibilità del database. È possibile eseguire operazioni di backup di copie di database attive e passive da qualsiasi server, tuttavia il ripristino può essere eseguito solo su una copia di database attiva.
- Exchange Server 2013: il backup e il ripristino del Servizio Copia Shadow del volume Microsoft (VSS) viene supportato. La tecnologia GRT (Granular Recovery Technology) non è supportata.

È possibile eseguire il ripristino dei dati Microsoft Exchange Server ai seguenti livelli:

- Writer Microsoft Exchange - Ripristina tutti i dati di Exchange Server.
- Gruppo di Archiviazione - Ripristina un gruppo di archiviazione specifico (non applicabile a Microsoft Exchange Server 2010).
- Archivio caselle di posta - Ripristina un archivio di casella di posta specifico (applicabile solamente a Microsoft Exchange Server 2003).
- Database delle caselle di posta - Ripristina un database delle caselle di posta specifico (applicabile a Exchange Server 2007 e 2010).

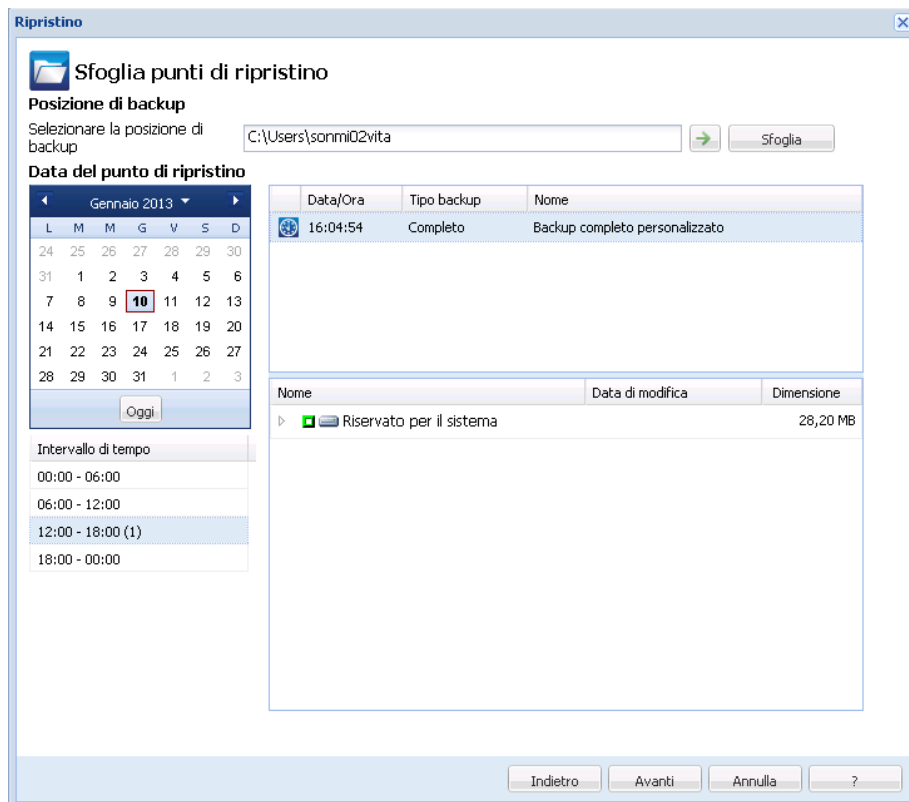
Nota: prima di procedere, eseguire i prerequisiti necessari indicati nella sezione Ripristini a livello di applicazione (a pagina 110).

Importante. Il ripristino degli elementi della casella di posta elettronica dell'utente di Microsoft Exchange Server non è supportato dalle sessioni di CA ARCserve Central Host-Based VM Backup. Per eseguire il ripristino dei dati Microsoft Exchange Server a livello granulare, è necessario eseguire il backup dei dati Exchange Server mediante CA ARCserve Central Protection Manager o CA ARCserve D2D.

Per ripristinare i dati del server Exchange

1. Verificare che CA ARCserve D2D sia installato sul sistema operativo guest.
2. Accedere al sistema operativo guest sul computer virtuale in cui si desidera eseguire il ripristino dei dati Exchange Server.
3. Avviare CA ARCserve D2D, quindi fare clic su Ripristina del riquadro Navigazione per aprire la finestra di dialogo Ripristina.
4. Fare clic su Sfoglia punti di ripristino per aprire la finestra di dialogo corrispondente.
5. Nel campo Selezionare la posizione di backup della finestra di dialogo Sfoglia punti di ripristino, specificare il percorso della sessione di backup del computer virtuale basato sull'host di cui si desidera eseguire il ripristino dei dati da Exchange Server. Il seguente percorso rappresenta un esempio del percorso di accesso alla sessione di backup del computer virtuale basato su host:

   ```
   https://<nome server>/<nome condivisione>/vm@<nome host o indirizzo IP del
   sistema server ESX>
   ```

6. Nel calendario, fare clic su una data e un'ora per il punto di ripristino.

7. Fare clic su Avanti per aprire la finestra di dialogo Opzioni di ripristino.

8. Selezionare la destinazione per il ripristino.

   Le opzioni disponibili consentono di eseguire il ripristino nella posizione originale di backup, nel gruppo di archiviazione di recupero, nel database delle caselle di posta di recupero oppure di eseguire il ripristino solo del file di dettagli.

   Ripristina in posizione originale

   Esegue il ripristino dei dati nella posizione originale di acquisizione dell'immagine di backup.

   Solo file di dettagli

   Esegue il ripristino dei file dei dettagli.

   CA ARCserve D2D esegue il ripristino del file di database di Microsoft Exchange nella cartella specificata, che rimarrà non in linea una volta completato il recupero. Sarà quindi possibile spostare il file in un server diverso e montarlo su Exchange Server manualmente per visualizzare i dati in esso contenuti.

   Nota: se è presente un database di elementi ripristinati da caselle di posta, il ripristino mediante l'opzione Solo file di dettagli non verrà completato.

Riproduci registro sul database

Con questa opzione, quando viene eseguito il dump dei file di database sulla cartella di destinazione, è possibile riprodurre ed applicare file di registro delle transazioni di Microsoft Exchange e confermarli nel file del database. Con il successivo avvio del database, i file di registro delle transazioni non ancora scritti sui file di database vengono applicati prima che il database sia nuovamente disponibile.

Nota: questa opzione non è applicabile per Microsoft Exchange Server 2003.

Ripristina sul gruppo di archiviazione di recupero (Exchange 2007)

Esegue il ripristino del database sul gruppo di archiviazione di recupero (RSG).

Un RSG è un gruppo di archiviazione che può essere utilizzato per operazioni di recupero. È possibile ripristinare i database delle caselle di posta di Microsoft Exchange Server da un backup in un gruppo di archiviazione di recupero, quindi recuperare ed estrarre i dati senza compromettere il database di produzione a cui accedono gli utenti finali.

- Se viene selezionato un singolo gruppo di archiviazione o database (ad eccezione dei database delle cartelle pubbliche) dallo stesso gruppo di archiviazione per il ripristino, la destinazione di ripristino predefinita corrisponderà a Ripristina sul gruppo di archiviazione di recupero oppure Ripristina sul database di recupero.
- Se più gruppi di archiviazione o database provenienti da più gruppi di archiviazione vengono selezionati per il ripristino, Exchange può essere ripristinato soltanto sulla posizione originale oppure mediante l'opzione Solo file di dettagli. La destinazione di ripristino predefinita è Ripristina in posizione originale.

Prima di eseguire il ripristino di un database Exchange 2007 su un Gruppo di archiviazione di recupero è necessario creare un gruppo di archiviazione di recupero ed un database delle caselle di posta con lo stesso nome.

Ad esempio, se si desidera ripristinare MailboxDatabase1 dal primo gruppo di archiviazione su un gruppo di archiviazione di recupero, è necessario creare un gruppo di archiviazione di recupero ed aggiungere il database MailboxDatabase1 al gruppo di archiviazione di recupero.

Nota: questa opzione non è applicabile per Microsoft Exchange Server 2003.

Smonta il database prima del ripristino e montalo dopo il ripristino.

In genere, prima di eseguire un ripristino, Microsoft Exchange verifica le seguenti condizioni:

- Lo stato del database da ripristinare è Smontato.
- Non è stato eseguito il ripristino imprevisto del database.

  Per evitare il ripristino imprevisto di un database di produzione di Microsoft Exchange, è disponibile un'opzione che consente di sovrascrivere il database durante il processo di ripristino. Nel caso in cui tale opzione sia disattivata, Microsoft Exchange non esegue il ripristino del database.

In CA ARCserve D2D, queste opzioni corrispondono all'opzione Smonta il database prima del ripristino e montalo dopo il ripristino. Questa opzione consente l'avvio automatico del processo di ripristino in modo automatico, senza dover eseguire alcuna operazione manuale. Se lo si desidera, è possibile impostare il montaggio/smontaggio manuale del database.

- Se selezionata, il processo di recupero smonta automaticamente il database di Exchange prima di avviare il processo di ripristino e monta il database una volta completato il processo di ripristino. Inoltre, questa opzione consente la sovrascrittura del database di Exchange durante il ripristino.
- Se deselezionata, il processo di recupero non smonta automaticamente il database di Exchange prima di avviare il processo di recupero e monta il database una volta completato il recupero.

  È necessario che l'amministratore di Exchange esegua alcune operazioni manuali, ad esempio smontare il database di Exchange, impostare il flag di sovrascrittura del database e montare il database di Exchange. La procedura di recupero viene eseguita da Exchange durante il montaggio del database.

  Inoltre, questa opzione non consente la sovrascrittura del database di Exchange durante il ripristino.

Ripristina sul database di recupero (Exchange 2010)

Esegue il ripristino del database su un database di recupero. Un database di recupero è un database che può essere utilizzato per operazioni di recupero. È possibile ripristinare i database delle caselle di posta di Microsoft Exchange Server da un backup su un database di recupero, quindi eseguire il recupero e l'estrazione dei dati senza compromettere il database di produzione a cui accedono gli utenti finali.

Prima di eseguire il ripristino di un database Exchange 2010 su un database di recupero, è necessario creare prima di tutto il database di recupero.

Nota: questa opzione non è applicabile ai database Microsoft Exchange Server 2003 e 2007.

9. Fare clic su Avanti per aprire la finestra di dialogo Riepilogo di ripristino.
10. Verificare che le opzioni di ripristino e le impostazioni siano corrette.
    - Se le informazioni di riepilogo non sono corrette, fare clic su Indietro e accedere alla finestra di dialogo corrispondente per modificare le impostazioni non corrette.
    - Se le informazioni di riepilogo sono corrette, fare clic su Fine per avviare il processo di ripristino.

Ripristino di dati SQL Server

È possibile eseguire ripristini a livello di applicazione dei dati Microsoft SQL Server con:

- Microsoft SQL Server 2005 Express, Standard, Workgroup ed Enterprise
- Microsoft SQL Server 2008, SQL Server 2008 R2 Express, Web, Standard, Workgroup ed Enterprise

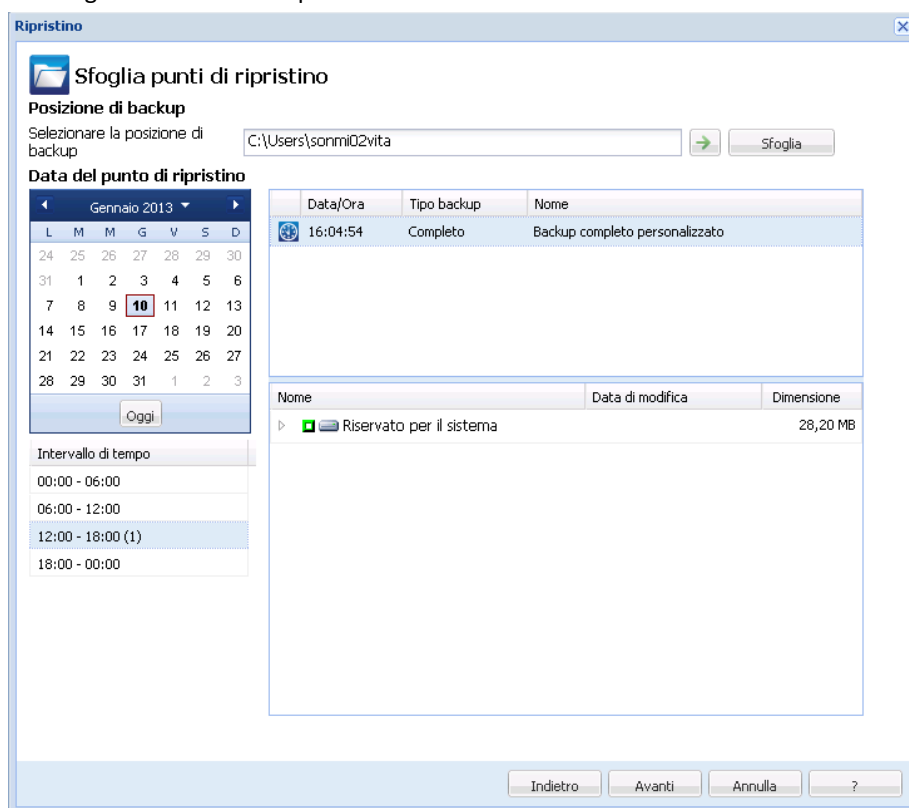
Nota: prima di procedere, prendere visione dei prerequisiti indicati nella sezione Ripristino a livello di applicazione (a pagina 110).

Importante. Il ripristino granulare di Microsoft SQL Server non funziona sulla console di CA ARCserve Central Host-Based VM Backup. Per ripristinare i dati di Microsoft SQL Server, installare CA ARCserve D2D sul computer virtuale guest.

Procedere come descritto di seguito:

1. Verificare che CA ARCserve D2D sia installato sul sistema operativo guest.
2. Accedere al sistema operativo guest del computer virtuale in cui si desidera eseguire il ripristino dei dati SQL Server.
3. Avviare CA ARCserve D2D, quindi fare clic su Ripristina del riquadro Navigazione per aprire la finestra di dialogo Ripristina.
4. Fare clic su Sfoglia punti di ripristino per aprire la finestra di dialogo corrispondente.
5. Nel campo Selezionare la posizione di backup della finestra di dialogo Sfoglia punti di ripristino, specificare il percorso della sessione di backup del computer virtuale basato sull'host di cui si desidera eseguire il ripristino dei dati da SQL Server. Il seguente percorso rappresenta un esempio del percorso di accesso alla sessione di backup del computer virtuale basato su host:

   ```
   https://<nome server>/<nome condivisione>/vm@<nome host o indirizzo IP del sistema server ESX>
   ```

6. Selezionare il punto di ripristino (data e ora)e selezionare il database Microsoft Exchange che si desidera ripristinare.

7. Fare clic su Avanti per aprire la finestra di dialogo Opzioni di ripristino.

   Selezionare la destinazione per il ripristino. Le opzioni disponibili consentono di eseguire il ripristino nella posizione originale del backup, in una posizione diversa oppure solo del file di dettagli.

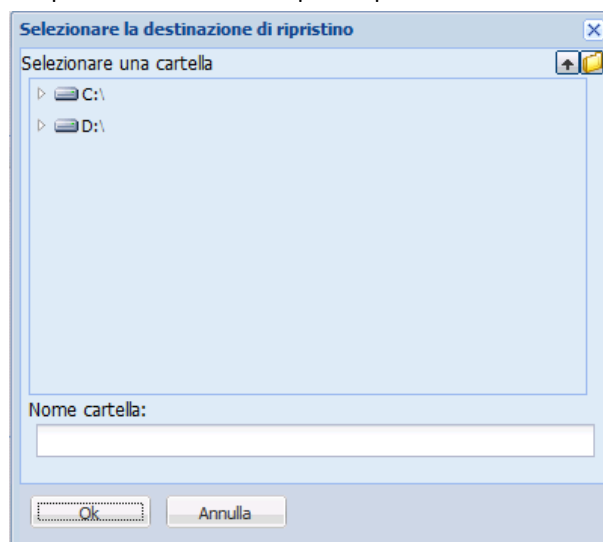
   Ripristina in posizione originale

   Esegue il ripristino dei dati nella posizione originale di acquisizione dell'immagine di backup.

   Solo file di dettagli

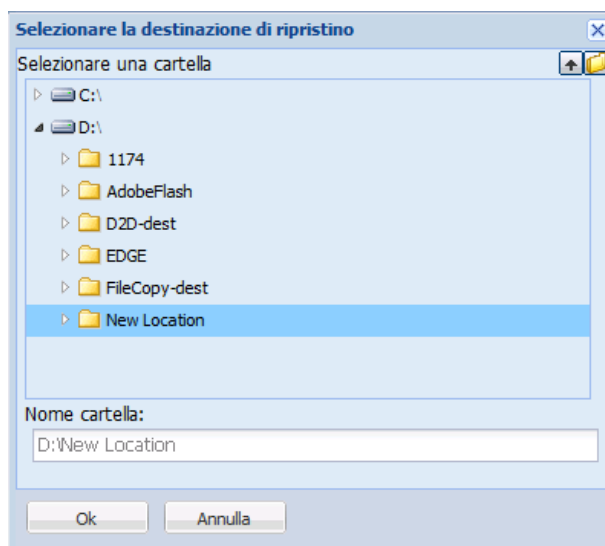
   Esegue il ripristino dei file dei dettagli.

   I file di dettagli vengono creati quando si verifica un arresto anomalo di un'applicazione. Contengono informazioni aggiuntive (indicazione data e ora) che possono essere utilizzate per la risoluzione dell'origine del problema.

   Quando si seleziona questa opzione, è possibile specificare o selezionare il percorso della cartella per il ripristino del file di dettagli.

   Ripristina in posizione alternativa

   Esegue il ripristino in un percorso alternativo (diverso dal percorso originale).

Nome istanza	Nome database	Nuovo nome database	Posizione file alternativa
ARCSERVE_APP	ARCAppDB	ARCAppDB	Sfoglia

I backup possono essere copiati in percorsi di rete, pertanto, possono essere utilizzati da più istanze SQL Server. È quindi possibile eseguire il ripristino di più database contemporaneamente a partire dal livello di istanza. L'elenco consente di selezionare l'istanza di database e di specificare un nuovo nome di database e un percorso alternativo per il ripristino del database. È inoltre possibile ricercare il percorso alternativo su cui eseguire il ripristino del database.

8. Fare clic su Avanti per aprire la finestra di dialogo Riepilogo di ripristino.
9. Verificare che le opzioni di ripristino e le impostazioni siano corrette.
   - Se le informazioni di riepilogo non sono corrette, fare clic su Indietro e accedere alla finestra di dialogo corrispondente per modificare le impostazioni non corrette.
   - Se le informazioni di riepilogo sono corrette, fare clic su Fine per avviare il processo di ripristino.

Capitolo 5: Risoluzione dei problemi di CA ARCserve Central Host-Based VM Backup

In questa sezione vengono fornite informazioni che consentono di identificare e risolvere i problemi che possono verificarsi durante l'utilizzo di CA ARCserve Central Host-Based VM Backup.

Questa sezione contiene i seguenti argomenti:

Messaggi di errore di connessione al server specificato durante il tentativo di aggiunta dei nodi.

Valido per piattaforme Windows.

Sintomo:

Quando si tenta di aggiungere o di stabilire la connessione a nodi dalla schermata Nodo, viene visualizzato il seguente messaggio di errore.

```
Impossibile connettersi al server specificato.
```

Soluzione:

Se tale messaggio viene visualizzato quando si tenta di aggiungere nodi dalla schermata Nodo, le seguenti azioni correttive possono contribuire alla risoluzione del problema:

- Verificare che il servizio Windows Server sia in esecuzione sul computer virtuale di origine (nodo) e sul server CA ARCserve Central Host-Based VM Backup.
- Assicurarsi che l'eccezione di Windows Firewall sia applicata al servizio di condivisione di file e stampanti di Windows sul computer virtuale di origine (nodo) e sul server CA ARCserve Central Host-Based VM Backup.
- Assicurarsi che un'eccezione di Windows Firewall sia applicata al servizio Netlogon di Windows solo se il nodo non è membro di un dominio. Eseguire questa attività sul server CA ARCserve Central Host-Based VM Backup e sul computer virtuale di origine (nodo).
- Verificare che il valore applicato al modello Condivisione e protezione per l'account locale sia Classico. Per applicare il valore Classico, procedere come segue:

  Nota: eseguire i seguenti passaggi sul computer virtuale di origine (nodo) e sul server CA ARCserve Central Host-Based VM Backup.

  1. Accedere al server CA ARCserve Central Host-Based VM Backup e aprire il pannello di controllo.
  2. Dal Pannello di controllo selezionare Strumenti di amministrazione.
  3. Fare doppio clic su Criteri di protezione locali.

     Verrà visualizzata la finestra di dialogo Criteri di protezione locali.

4. Dalla finestra Criteri di protezione locali, espandere Criteri locali e Opzioni di protezione.

   Verranno visualizzati i criteri di protezione.

5. Fare clic con il pulsante destro del mouse su Accesso alla rete: modello di condivisione e protezione per gli account locali e scegliere Proprietà dal menu di scelta rapida.

   Verrà visualizzata la finestra delle proprietà Accesso alla rete: modello di condivisione e protezione per gli account locali.

6. Fare clic su Impostazioni di protezione locali.

   Dall'elenco a discesa, selezionare Classico: gli utenti locali effettuano l'autenticazione di se stessi.

   Fare clic su OK.

- Verificare che il valore applicato ai criteri locali per il livello di autenticazione del manager della rete LAN sia impostato su invia LM & NTLMv2 – utilizza la protezione di sessione NTLMv2 se negoziata. Per applicare il valore, eseguire le seguenti operazioni:

  1. Accedere al server CA ARCserve Central Host-Based VM Backup e aprire il prompt dei comandi.

     Eseguire il seguente comando

     ```
     secpol.msc
     ```

     Verrà visualizzata la finestra di dialogo Impostazioni protezione locale.

  2. Selezionare i criteri locali e fare clic sulle opzioni di protezione.

     Ricerca di protezione di rete: livello di autenticazione di manager rete LAN.

     Fare doppio clic sull'opzione.

     Verrà visualizzata la finestra di dialogo Proprietà.

  3. Selezionare l'opzione seguente e fare clic su OK.

     ```
     invia LM & NTLMv2 – utilizza la protezione di sessione NTLMv2 se negoziata.
     ```

  4. Dal prompt dei comandi, eseguire il comando riportato di seguito:

     ```
     gpupdate
     ```

  Il valore viene applicato.

Pagine Web vuote o errori Javascript.

Valido sui sistemi operativi Windows Server 2008 e Windows Server 2003.

Sintomo:

Quando i siti Web di CA ARCserve Central Applications vengono aperti utilizzando Internet Explorer, vengono visualizzate pagine Web vuote oppure si verificano errori Javascript. Il problema si verifica quando si apre Internet Explorer sui sistemi operativi Windows Server 2008 e Windows Server 2003.

Questo problema si verifica nei seguenti casi:

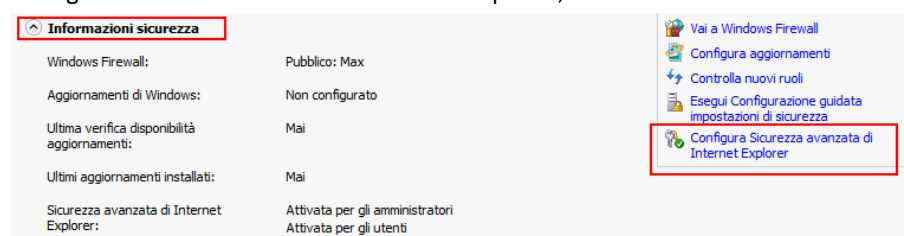
- Quando si utilizza Internet Explorer 8 o Internet Explorer 9 per visualizzare l'applicazione e il browser non riconosce l'URL come sito attendibile.
- Quando si utilizza Internet Explorer 9 per visualizzare l'applicazione e il protocollo di comunicazione in uso è HTTPS.

Soluzione:

Per risolvere il problema, disattivare la protezione avanzata di Internet Explorer sui computer utilizzati per visualizzare l'applicazione.

Per disattivare la protezione avanzata di Internet Explorer su sistemi Windows Server 2008, procedere come segue:

1. Accedere al computer Windows Server 2008 utilizzato per visualizzare i rapporti utilizzando l'account di amministratore o un account che dispone di privilegi amministrativi.
2. Fare clic con il pulsante destro su Computer sul desktop e scegliere Gestisci per aprire la finestra di Server Manager.
3. Dalla finestra Server manager fare clic su Server Manager (nome server).

   Dalla sezione Riepilogo server, aprire Informazioni di protezione e fare clic su Configura Protezione avanzata di Internet Explorer, come illustrato a continuazione:

   Viene visualizzata la finestra di dialogo Protezione avanzata di Internet Explorer.

4. Nella finestra di dialogo Protezione avanzata di Internet Explorer, procedere come segue:
   - Disattiva il controllo Administrators--Click
   - Disattiva il controllo Users--Click

   Fare clic su OK.

La finestra di dialogo Protezione avanzata di Internet Explorer viene chiusa e la protezione di Internet Explorer viene disabilitata.

Per disattivare la protezione avanzata di Internet Explorer su sistemi Windows Server 2003, procedere come segue:

1. Accedere al computer Windows Server 2003 utilizzato per visualizzare i rapporti utilizzando l'account di amministratore o un account che dispone di privilegi amministrativi.
2. Aprire il Pannello di controllo di Windows, quindi aprire Installazione applicazioni.
3. Dalla finestra di dialogo Installazione applicazioni selezionare l'opzione Installazione componenti di Windows per avviare l'Aggiunta guidata componenti di Windows.

   Eliminare il segno di spunta accanto a Protezione avanzata di Internet Explorer.

   Fare clic su Avanti.

   Proseguire seguendo le istruzioni visualizzate per completare l'installazione, quindi fare clic su Fine.

La protezione avanzata di Internet Explorer è disabilitata.

Le pagine Web non vengono caricate correttamente quando si accede ai nodi CA ARCserve D2D

Valido per piattaforme Windows.

Sintomo:

Le pagine Web non vengono caricate correttamente nel browser e/o vengono visualizzati messaggi di errore quando si accede ai nodi CA ARCserve D2D dalla schermata Nodi.

Soluzione:

Questo comportamento interessa principalmente i browser Internet Explorer. È possibile che le pagine Web non vengano caricate correttamente quando l'esecuzione script, i controlli ActiveX o i programmi Java sono disabilitati nel computer o bloccati sulla rete.

Per risolvere il problema, aggiornare la finestra del browser. Se il problema persiste dopo l'aggiornamento della finestra del browser, procedere come segue:

1. Aprire Internet Explorer.

   Scegliere Opzioni Internet dal menu Strumenti.

   Verrà visualizzata la finestra di dialogo Opzioni Internet.

2. Fare clic sulla scheda Protezione.

   Vengono visualizzate le opzioni di sicurezza.

3. Fare clic sull'area Internet.

   Vengono visualizzate le opzioni relative all'area Internet.

4. Fare clic su Livello personalizzato.

   Viene visualizzata la finestra di dialogo Impostazioni di sicurezza - Area Internet.

5. Scorrere fino alla categoria Esecuzione script.

   individuare Esecuzione script attivo.

   Selezionare l'opzione Attiva o Chiedi conferma.

6. Fare clic su OK nella finestra di dialogo impostazioni di sicurezza - Area Internet.

   La finestra di dialogo Impostazioni di sicurezza - Area Internet viene chiusa.

7. Fare clic su OK nella finestra di dialogo Opzioni Internet.

   La finestra di dialogo Opzioni Internet viene chiusa e l'opzione di esecuzione script attivo viene applicata.

Nota: se il problema non viene risolto, contattare l'amministratore di sistema per verificare che altri programmi, ad esempio programmi antivirus o firewall, non blocchino l'esecuzione degli script attivi, i controlli ActiveX o i programmi Java.

Risoluzione dei problemi relativi al caricamento delle pagine

Valido per piattaforme Windows.

Sintomo:

La finestra del browser visualizza i messaggi di errore riportati di seguito quando viene eseguito l'accesso ai nodi CA ARCserve Central Applications e CA ARCserve D2D e ai server di monitoraggio.

Messaggio 1:

`Gli errori presenti nella pagina Web potrebbero impedirne il corretto funzionamento.`

Messaggio 2:

`!`

Soluzione:

Il caricamento delle pagine Web non viene eseguito correttamente per diverse ragioni. Nella tabella seguente sono descritte le cause più comuni e le corrispondenti misure correttive:

Motivo	Misura correttiva
Si sono verificati problemi relativi al codice sorgente HTML sottostante.	Aggiornare la pagina Web e riprovare.
La rete blocca l'esecuzione degli script attivi, i controlli ActiveX o i programmi Java.	Consentire al browser di utilizzare gli script attivi, i controlli ActiveX o i programmi Java.
L'applicazione antivirus è configurata per la scansione dei file temporanei Internet e dei programmi scaricati.	Applicare un filtro nell'applicazione antivirus in modo da consentire i file Internet associati alle pagine Web di CA ARCserve Central Applications.
Il motore di script installato nel computer è danneggiato o non è aggiornato.	Aggiornare il motore di script.
I driver della scheda video installati nel computer sono danneggiati o non sono aggiornati.	Aggiornare i driver della scheda video.
Il componente DirectX installato nel computer è danneggiato o non è aggiornato.	Aggiornare il componente DirectX.

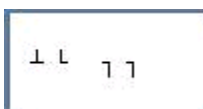
Visualizzazione di caratteri corrotti nella finestra del browser durante l'accesso a CA ARCserve Central Applications

Valido per tutti i sistemi operativi Windows e per tutti i browser.

Sintomo:

Quando viene eseguito l'accesso a CA ARCserve Central Applications, vengono visualizzati caratteri corrotti nell'area di contenuto della finestra del browser.

Soluzione:

Questo problema si verifica nel caso in cui l'installazione di CA ARCserve Central Applications sia stata eseguita mediante comunicazione HTTPS e l'accesso a CA ARCserve Central Applications mediante comunicazione HTTP. Il componente dei servizi Web sottostanti di CA ARCserve Central Applications non supporta la funzionalità di conversione degli URL HTTP in HTTPS. Di conseguenza, i caratteri corrotti vengono visualizzati nella finestra del browser. Ad esempio:

Per correggere il problema, accedere a CA ARCserve Central Applications utilizzando il protocollo HTTPS per l'installazione o la configurazione delle applicazioni di comunicazione che utilizzano tale protocollo.

Errore di accesso negato durante l'aggiornamento dei nodi

Valido su tutti i sistemi operativi Windows con supporto del Controllo account utente (UAC).

Nota: Windows Vista o versioni successive.

Sintomo 1:

Se l'account utente di Windows specificato non corrisponde a un account predefinito di amministratore o a un account utente di dominio e appartiene al gruppo di amministratori, quando l'utente introduce la password nella finestra di dialogo Credenziali nodo della finestra Importa computer virtuali da vCenter/ESX, viene visualizzato il messaggio seguente:

`È necessario disporre dei privilegi di amministratore.`

In tal caso non sarà possibile applicare le credenziali del nodo.

Sintomo 2:

Se l'operazione di importazione dei nodi viene eseguita senza specificare le credenziali del nodo, quando l'utente tenta di eseguire l'operazione di aggiornamento del nodo con un account che non corrisponde a un account predefinito di amministratore o a un account utente di dominio e appartiene al gruppo di amministratori, viene visualizzato il messaggio seguente:

`Accesso negato. Verificare di disporre dei privilegi di amministratore e che l'accesso al registro di sistema remoto non sia limitato dai criteri di protezione locali del computer aggiunto.`

In tal caso non sarà possibile aggiornare il nodo.

Soluzione:

Si tratta di un comportamento previsto in caso di abilitazione del Controllo account utente (UAC) su un computer con sistema operativo Windows e supporto UAC. Il Controllo dell'account utente è una funzionalità Windows che consente l'accesso remoto al computer solo agli utenti con diritti di amministratore.

Per risolvere il problema, procedere secondo una delle modalità riportate a continuazione:

- Fornire le credenziali integrate o dell'amministratore di dominio.
- Disabilitare il Controllo dell'account utente:
    1. Accedere al nodo utilizzando l'account amministratore.
    2. Aprire il Pannello di controllo di Windows.
    3. Aprire Account utente.
    4. Nella schermata Modifica dell'account utente, fare clic su Modifica impostazioni di Controllo dell'account utente ed eseguire una delle operazioni seguenti:
        - **Windows Vista e Windows Server 2008:** nella schermata Modifica dell'account utente, fare clic su Attiva o disattiva Controllo account utente. Nella sezione Per aumentare la protezione del computer e renderlo più sicuro, attivare il controllo dell'account utente, deselezionare la casella di controllo accanto Per proteggere il computer, utilizzare il controllo dell'account utente e fare clic su OK.

          Riavviare il computer per applicare le modifiche apportate al Controllo dell'account utente.
        - **Windows Server 2008 r2 e Windows 7:** nella schermata Scegliere quando ricevere la notifica delle modifiche al computer, spostare l'Indicatore scorrevole da Notifica sempre a Non notificare mai. Fare clic su OK e chiudere il Pannello di controllo di Windows.

          Riavviare il computer per applicare le modifiche apportate al Controllo dell'account utente.

Viene visualizzato un errore del certificato quando si accede all'applicazione

Valido per piattaforme Windows.

Sintomo:

Quando si accede all'applicazione viene visualizzato il seguente messaggio nella finestra del browser:

- Internet Explorer

  `Si è verificato un problema con il certificato di protezione del sito Web.`

- Firefox

  `Questa connessione non è attendibile.`

- Chrome:

  `Il certificato di sicurezza di questo sito non è attendibile.`

Se si specifica un'opzione che consente di passare al sito Web, sarà possibile accedere all'applicazione. Questo comportamento, tuttavia, si verifica ogni volta che si accede all'applicazione.

Soluzione:

Questo comportamento si verifica quando si imposta l'utilizzo di HTTPS come protocollo di comunicazione. Per risolvere temporaneamente il problema, nella finestra del browser fare clic sul collegamento che consente di passare al sito Web. Al successivo accesso all'applicazione, comunque, il messaggio verrà nuovamente visualizzato.

Il protocollo di comunicazione HTTPS (sicuro) garantisce una maggiore sicurezza rispetto al protocollo di comunicazione HTTP. Se si desidera continuare a comunicare utilizzando il protocollo di comunicazione HTTPS, è possibile acquistare un certificato di sicurezza da VeriSign e quindi installare il certificato sul server applicazioni. Facoltativamente, è possibile impostare su HTTP il protocollo di comunicazione utilizzato dall'applicazione. Per impostare il protocollo di comunicazione su HTTP, procedere come segue:

1. Accedere al server in cui è installata l'applicazione.
2. Individuare la seguente directory:

   `C:\Programmi\CA\ARCserve Central Applications\BIN`

3. Eseguire il file batch seguente:

   `ChangeToHttp.bat`

4. Al termine dell'esecuzione del file batch, aprire Server Manager di Windows.

   Riavviare il seguente servizio:

   `Servizio CA ARCserve Central Applications`

Errori di backup con errori di creazione della snapshot

Valido per piattaforme Windows.

Quando vengono inviati backup per computer virtuali VMware, si verificano i seguenti sintomi:

Sintomo 1

I processi di backup di computer virtuale producono un errore e nel Registro attività viene visualizzato il seguente messaggio:

```
Impossibile acquisire la snapshot. Errore dei rapporti ESX/vCenter. Si è verificato un errore generale di sistema. Errore di protocollo da VMX.
```

Soluzione 1

Si tratta di un problema VMware. Per correggere il problema, disinstallare e reinstallare gli strumenti VMware nel sistema operativo guest, quindi inoltrare nuovamente il processo.

Sintomo 2

I processi di backup di computer virtuale producono un errore e nel Registro attività viene visualizzato il seguente messaggio:

```
Impossibile acquisire la snapshot del computer virtuale. Il server ESX/vCenter riporta un errore di creazione della snapshot inattiva dovuto a un tempo di attesa eccessivo dei dati di I/O dell'operazione di creazione snapshot sul computer virtuale bloccato.
```

Soluzione 2

Questo errore si verifica quando VSS rileva errori durante la creazione di snapshot. Il servizio VSS può rilevare errori se si verificano le seguenti condizioni:

Un writer VSS indica uno stato instabile.

Per determinare l'origine del problema e correggere il comportamento, eseguire le seguenti azioni:

1. Eseguire il comando "vssadmin list writers" dalla riga di comando del sistema operativo guest del computer virtuale.
2. Verificare che tutti i writer VSS indichino uno stato corretto.
3. Se esistono writer che indicano uno degli stati seguenti, contattare Microsoft o il fornitore del writer per ottenere informazioni sulla correzione degli errori.

   ```
   state=Failed
   Last Error=No Error
   ```

   Nota: il riavvio dei writer consente solitamente di risolvere il problema.

VSS ha rilevato errori durante la creazione di snapshot.

Per determinare l'origine del problema e correggere il comportamento, eseguire le seguenti azioni:

1. Verificare il registro eventi di Windows nel sistema operativo guest. Verificare gli errori relativi ai componenti VSS dopo l'avvio del backup.
2. Quando VSS segnala errori dovuti a spazio su disco insufficiente, sarà necessario liberare spazio su disco del volume associato all'errore.
3. Se il servizio VSS o il driver Windows Volsnap generano errori di timeout, le applicazioni in esecuzione sul computer virtuale saranno altamente attive. Tale stato impedisce la creazione di snapshot coerenti. Per ovviare a questa condizione, pianificare i backup nei periodi in cui le applicazioni eseguono meno operazioni di immissione e output nel volume.
4. Se il registro eventi di Windows indica che il driver di VolSnap ha rilevato errori, consultare l'articolo Volume Snapshot Driver Integrity disponibile nella libreria Microsoft Technet per ottenere informazioni sulla correzione degli errori VolSnap.

Errore sconosciuto delle operazioni di recupero del computer virtuale

Applicabile ai sistemi operativi Windows.

Sintomo:

Errore delle operazioni di recupero del computer virtuale È possibile inoltrare il processo di recupero del computer virtuale, tuttavia nel Registro attività verrà visualizzato il messaggio seguente:

```
Impossibile recuperare i dischi virtuali.
```

Inoltre, VDDK riporta il seguente messaggio di errore:

```
Errore sconosciuto.
```

Soluzione 1:

Per risolvere il problema, considerare quanto segue:

- Le operazioni di recupero dei computer virtuali non vengono completate poiché l'archivio dati originale non dispone di spazio sufficiente. VDDK restituisce questo messaggio in quanto l'API di VDDK non supporta la funzionalità che consente di rilevare la quantità di spazio disponibile sul disco dell'archivio dati originale. L'archivio dati è la posizione in cui è stato specificato il recupero del computer virtuale. Per risolvere il problema, liberare lo spazio su disco necessario nell'archivio dati originale per il completamento dell'operazione, quindi rinviare il processo.
- I disturbi di rete ed un traffico di rete elevato possono comportare un errore dei processi di recupero del computer virtuale. Per risolvere il problema, verificare che il server proxy e i sistemi Server ESX o vCenter siano in grado di comunicare attraverso la rete, quindi inviare nuovamente il processo.
- Possono verificarsi errori dovuti a connessioni multiple simultanee di processi di backup o recupero di computer virtuali verso sistemi server ESX o vCenter, comprese le connessioni vSphere SDK mediante il client VMware vSphere. Per correggere il problema, chiudere le connessioni non necessarie e inviare nuovamente il processo. Per informazioni circa la quantità massima di connessioni simultanee consentite, consultare la sezione Impossibile aprire il file VMDK (a pagina 150).
- Esaminare le sezioni Attività ed Eventi del log client VMware vSphere per rilevare errori interni per un computer virtuale specifico. Correggere gli errori interni e inviare nuovamente il processo.

  Esempio: il file VMDK è utilizzato da un'altra applicazione o un'altra operazione. Per risolvere il problema, rilasciare il file e inviare nuovamente il processo.

Soluzione 2:

Questo problema può verificarsi nei seguenti casi:

- VDDK non ha elaborato una snapshot correttamente.
- VDDK non ha eliminato una snapshot manualmente o interna al computer virtuale.

Per risolvere il problema, inviare nuovamente il processo. Se il processo produce nuovamente un errore, eliminare il computer virtuale di cui è stato eseguito il recupero e inviare nuovamente il processo.

Errore di montaggio dei dischi in modalità trasporto hotadd delle operazioni di backup e recupero

Valido per piattaforme Windows.

Sintomo:

I processi di backup e recupero che utilizzano la modalità di trasporto hotadd non sono in grado di eseguire il montaggio dei dischi sul sistema proxy.

Soluzione:

Per risolvere il problema, procedere come segue:

1. Aprire il client VMware vSphere.

   Accedere al sistema server ESX o al sistema server vCenter mediante le credenziali di amministratore.

2. Selezionare il computer virtuale proxy e modificare le impostazioni per il computer virtuale proxy.
3. Rimuovere i dischi hotadd allegati al computer virtuale di origine o al computer virtuale proxy.
4. Inoltrare nuovamente il processo.

Errore delle operazioni di recupero durante il recupero dei dati mediante la modalità di trasporto HOTADD o SAN

Valido per piattaforme Windows.

Sintomo:

Errore delle operazioni di recupero durante il recupero dei dati mediante la modalità di trasporto HOTADD o SAN. Il seguente messaggio viene visualizzato nel Registro attività:

```
Si è verificato un errore sconosciuto. Contattare il Supporto Tecnico.
```

Soluzione:

Errore delle operazioni di recupero con la modalità di trasporto HOTADD (a pagina 203) o SAN (a pagina 203) quando le impostazioni del disco non sono configurate correttamente.

Per configurare l'operazione il disco, procedere come segue:

1. Accedere al sistema proxy di backup mediante un account con privilegi di amministratore.
2. Aprire la riga di comando di Windows.
3. Dalla riga di comando, immettere il seguente comando:

   ```
   diskpart
   ```

   Premere Invio.
4. Digitare SAN, quindi premere Invio.

   Vengono visualizzati i criteri SAN correnti.
5. Digitare il seguente comando:

   ```
   SAN POLICY = OnlineAll
   ```

   Premere Invio.

   Il criterio SAN viene configurato in modo da non eseguire il montaggio automatico dei volumi SAN.
6. Per cancellare l'attributo di sola lettura di un determinato disco SAN, selezionare il disco dall'elenco, quindi immettere il seguente comando:

   ```
   attribute disk clear readonly
   ```

   Premere Invio.
7. Digitare exit, quindi premere Invio.

Il disco viene configurato e sarà possibile inoltrare nuovamente il processo.

Se il processo riporta errori ancora una volta, montare i dischi HOTADD manualmente utilizzando la gestione disco sul sistema proxy.

Per montare i dischi manualmente, procedere come segue:

1. Accedere al sistema proxy di backup mediante un account con privilegi di amministratore.
2. Aprire il Pannello di controllo di Windows e fare doppio clic su Strumenti di amministrazione.

   Viene visualizzata la finestra di dialogo degli strumenti di amministrazione.
3. Dall'elenco Preferiti, fare doppio clic su Gestione computer.

   Viene visualizzata la finestra della Gestione computer.

4. Espandere Archiviazione, quindi fare clic sulla Gestione disco.

   Vengono visualizzati i dischi.

5. Fare clic con il tasto destro del mouse sul disco che si desidera montare, quindi fare clic su In linea.

Il disco viene montato e sarà possibile inoltrare nuovamente il processo.

Sistema operativo non trovato

Valido per piattaforme Windows.

Sintomo 1

Quando il sistema operativo guest viene avviato su un computer virtuale dopo aver eseguito il recupero del computer virtuale mediante l'opzione Ripristina in posizione alternativa, viene visualizzato il seguente messaggio di errore:

```
Sistema operativo non trovato.
```

Soluzione 1

Il comportamento descritto può inoltre verificarsi su computer virtuali contenenti periferiche SCSI e IDE. Se il problema si verifica, verificare la configurazione dei dischi sul computer virtuale e accertarsi che la sequenza di avvio del computer virtuale di cui è stato eseguito il recupero corrisponda all'origine del computer virtuale. Se la sequenza di avvio è differente, sarà necessario aggiornare il BIOS del computer virtuale di cui è stato eseguito il recupero corrispondente all'origine.

Nota: Il primo disco IDE deve utilizzare (0:1).

Sintomo 2

Il seguente messaggio viene visualizzato quando il sistema operativo guest viene avviato su un computer virtuale dopo il recupero del computer virtuale:

```
Sistema operativo non trovato.
```

Soluzione 2

Se il problema si verifica, verificare la configurazione dei dischi sul computer virtuale e accertarsi che la sequenza di avvio del computer virtuale di replica corrisponda all'origine del computer virtuale.

Le modifiche all'indirizzo MAC non vengono memorizzate dopo il ripristino del computer virtuale

Valido per piattaforme Windows.

Sintomo:

Gli indirizzi MAC di computer virtuali non vengono mantenuti dopo il recupero di computer virtuali.

Soluzione:

Gli indirizzi MAC non vengono mantenuti durante il ripristino per evitare la presenza di duplicati. Per mantenere le informazioni relative all'indirizzo MAC, impostare la seguente chiave di registro sul server proxy:

```
Posizione: SOFTWARE\CA\CA ARCSERVE D2D
Nome chiave: RetainMACForVDDK
Tipo di valore: Stringa
Valore chiave: 1
```

Su computer virtuali con due schede NIC, impostare la chiave di registro RetainMACForVDDK se si desidera impostare una scheda su Manuale. In caso contrario, tutte le schede vengono impostate su Automatico dopo il recupero.

Errore del servizio Web di CA ARCserve D2D su nodi CA ARCserve D2D

Valido per piattaforme Windows.

Sintomo:

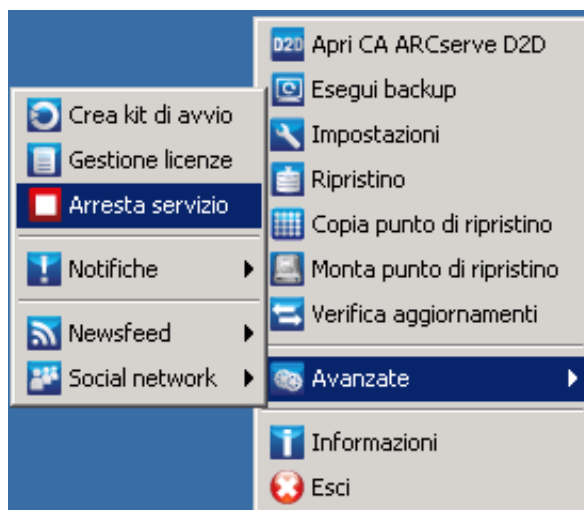
Il servizio Web in esecuzione sui nodi CA ARCserve D2D viene avviato e successivamente produce un errore oppure non viene avviato.

Soluzione:

Il problema si verifica quando la porta utilizzata dal servizio Web di CA ARCserve D2D coincide con quella utilizzata dal servizio Web VMware vCenter (Tomcat).

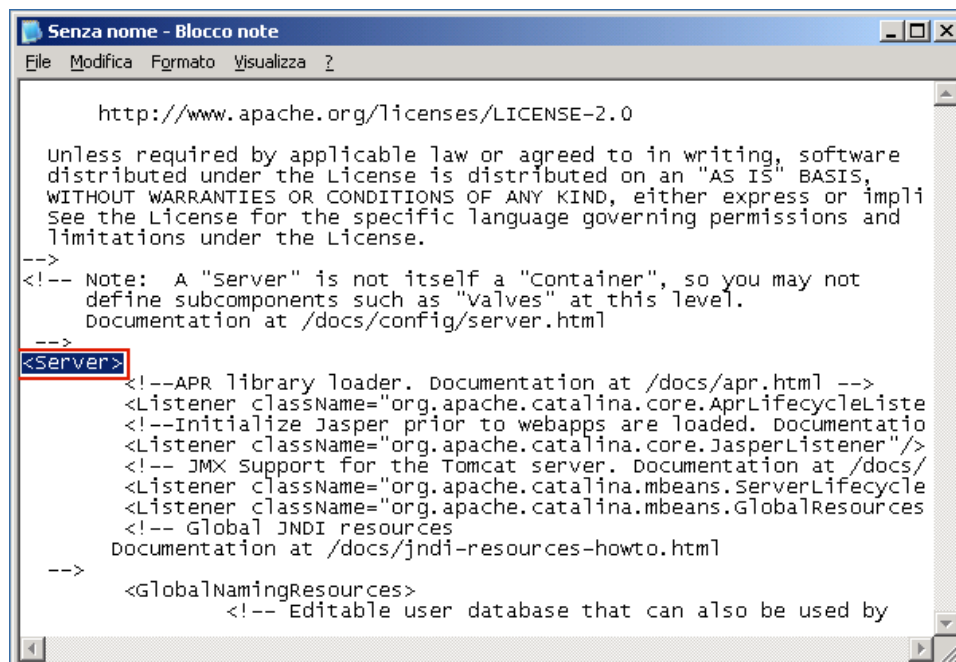
La porta utilizzata da CA ARCserve D2D potrebbe essere in conflitto con la porta predefinita utilizzata da Tomcat. In tal caso, se il server Tomcat viene avviato prima di CA ARCserve D2D potrebbero verificarsi errori. Per risolvere il problema, modificare la porta predefinita di Tomcat nel seguente modo:

1. Accedere a Computer di monitoraggio CA ARCserve D2D, fare clic sull'opzione Avanzate e selezionare Interrompi servizio.

   Il servizio Web di CA ARCserve D2D viene interrotto.

2. Aprire il file server.xml di Tomcat per modificare o configurare il comportamento di Tomcat.

   Il file server.xml di Tomcat è disponibile nel seguente percorso:

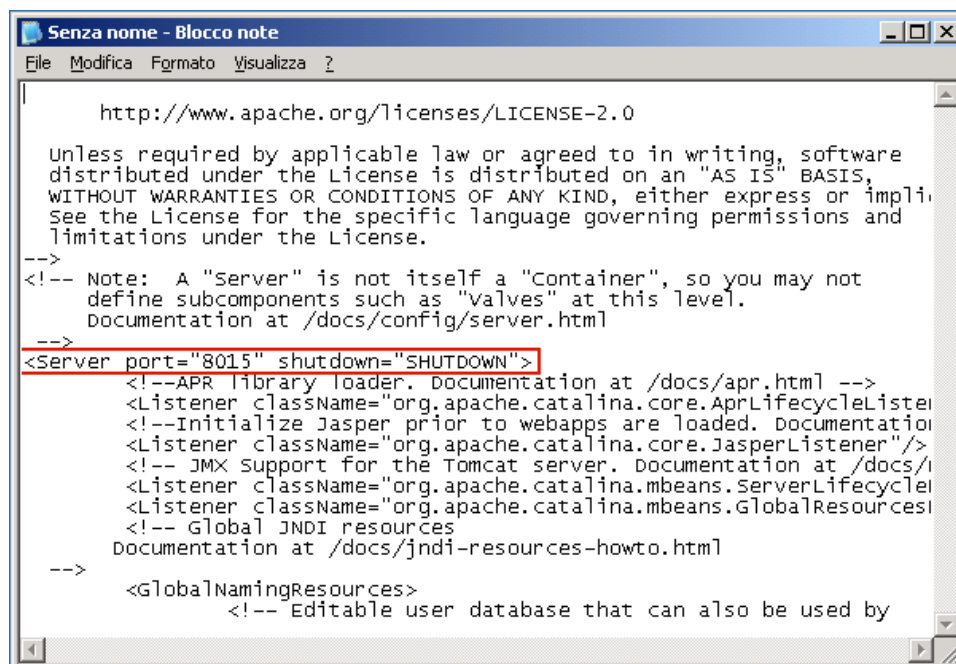
   `C:\Programmi\CA\ARCserve Central Applications\TOMCAT\conf`

3. Individuare il tag <Server> nel file server.xml.

4. Modificare il tag <Server> nel seguente modo:

   Da:

   <Server>

   A:

   <Server port="8015" shutdown="SHUTDOWN">

5. Salvare e chiudere il file server.xml.

   Il comando di arresto del server Tomcat viene configurato per essere ricevuto dal server attraverso la porta specificata (8015).

6. Accedere a Computer di monitoraggio CA ARCserve D2D, fare clic sull'opzione Avanzate e selezionare Avvia servizio.

   Il servizio Web di CA ARCserve D2D viene avviato.

Errore di comunicazione tra CA ARCserve Central Host-Based VM Backup e il servizio Web di CA ARCserve D2D sui nodi remoti

Applicabile ai sistemi operativi Windows.

Sintomo:

CA ARCserve Central Host-Based VM Backup non è in grado di stabilire la comunicazione con il servizio Web di CA ARCserve D2D sui nodi remoti.

Soluzione:

La tabella riportata di seguito descrive i motivi per i quali CA ARCserve Central Host-Based VM Backup non è in grado di comunicare con il servizio Web di CA ARCserve D2D su nodi remoti e l'azione correttiva corrispondente:

Causa	Misura correttiva
La rete non è disponibile o non è stabile durante l'applicazione dei criteri.	Verificare che la rete sia disponibile e stabile e riprovare.
Il computer di CA ARCserve D2D non è in grado di gestire il carico quando l'applicazione tenta di stabilire la comunicazione con il nodo.	Verificare che lo stato della CPU sul nodo di CA ARCserve D2D si normalizzi e riprovare.
Durante la distribuzione dei criteri, il servizio CA ARCserve D2D non è in esecuzione sul nodo remoto.	Verificare che CA ARCserve D2D sia in esecuzione sul nodo remoto e riprovare.
Si verificano problemi di comunicazione del servizio CA ARCserve D2D.	Riavviare il servizio CA ARCserve D2D sul nodo remoto e riprovare.

Lentezza di esecuzione del servizio Web di CA ARCserve D2D

Applicabile ai sistemi operativi Windows.

Sintomo 1:

L'esecuzione del servizio Web di CA ARCserve D2D su sistemi CA ARCserve D2D è lenta. È possibile individuare altri sintomi quali:

- Il servizio Web di CA ARCserve D2D non risponde o occupa il 100% delle risorse della CPU.
- Prestazioni insufficienti o errore di comunicazione dei nodi di CA ARCserve D2D con il servizio Web.

Soluzione 1:

In alcune configurazioni di ambiente, il servizio Web di CA ARCserve D2D richiede tempi di CPU troppo lunghi oppure presenta un ritardo nella risposta. Per impostazione predefinita, Tomcat è configurato per allocare un valore limitato di memoria ai nodi, impostazione che potrebbe non essere adatta all'ambiente in uso. Per verificare questo problema, consultare i seguenti file di registro:

```
<D2D_home>\TOMCAT\logs\casad2dwebsvc-stdout.*.log
<D2D_home>\TOMCAT\logs\casad2dwebsvc-stder.*.log
<D2D_home>\TOMCAT\logs\catalina.*.log
<D2D_home>\TOMCAT\logs\localhost.*.log
```

Individuare il seguente messaggio:

```
java.lang.OutOfMemoryError
```

Per correggere il problema, aumentare il valore di memoria allocata.

Per aumentare la memoria, eseguire le operazioni riportate di seguito:

1. Aprire l'Editor del Registro di sistema e selezionare la seguente chiave:
   - Sistemi operativi x86:

     ```
     HKEY_LOCAL_MACHINE\SOFTWARE\Apache Software Foundation\Procrun 2.0\CASAD2DWebSvc\Parameters\Java
     ```
   - Sistemi operativi x64:

     ```
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\CASAD2DWebSvc\Parameters\Java
     ```

2. Eseguire una delle seguenti operazioni:

   ■ Se il messaggio presente nel file di registro è il seguente:

     `java.lang.OutOfMemoryError: PermGen space`

     Aggiungere la stringa seguente al valore di Opzioni.

     `-XX:PermSize=128M -XX:MaxPermSize=128M`

     Nota: potrebbe essere necessario aumentare il valore di -XX:MaxPermSize per adattarlo al proprio ambiente.

   ■ Se il messaggio presente nel file di registro è uno dei seguenti:

     ```
     java.lang.OutOfMemoryError: Java heap space
     java.lang.OutOfMemoryError: GC overhead limit exceeded
     ```

     Aumentare il valore del seguente DWORD:

     `JvmMx`

3. Riavviare il servizio Web di CA ARCserve D2D.

Sintomo 2

I backup pianificati vengono ignorati e ne viene interrotta l'esecuzione.

Soluzione 2

Quando il valore massimo configurato corrisponde a 20 backup simultanei (o un valore inferiore), eseguire le seguenti operazioni:

1. Aumentare il valore del seguente DWORD:

   `JvmMx=256`

   Nota: il valore DWORD viene riportato nella soluzione 1.

2. Aggiungere la stringa seguente al valore di Opzioni.

   `-XX:MaxPermSize=128M`

   Nota: il valore DWORD viene riportato nella soluzione 1.

Quando il valore massimo configurato è compreso tra 20 e 50 backup simultanei, eseguire le seguenti operazioni:

1. Aumentare il valore del seguente DWORD:

   `JvmMx=512`

   Nota: il valore DWORD viene riportato nella soluzione 1.

2. Aggiungere la stringa seguente al valore di Opzioni.

   `-XX:MaxPermSize=256M`

   Nota: il valore DWORD viene riportato nella soluzione 1.

Errori della funzionalità di traccia dei blocchi modificati

Valido per Windows

Sintomo:

I backup dei computer virtuali generano errori e la funzionalità di traccia dei blocchi modificati è abilitata sui computer virtuali.

Soluzione:

La tabella seguente descrive le condizioni che possono determinare un errore di backup dei computer virtuali se la funzionalità di traccia dei blocchi modificati è abilitata:

Condizione	Soluzione
Le snapshot generate dall'utente sono presenti sui computer virtuali e la funzionalità di traccia dei blocchi modificati non è abilitata.	Abilitare o ripristinare la funzionalità di traccia dei blocchi modificati per consentire il processo di backup completo. **Nota**: il processo di backup completo procede con blocchi utilizzati e inutilizzati di dati dai file di VMDK.
La versione non corretta dell'hardware VMware è installata sul computer virtuale.	Verificare che la versione hardware di VMware 7.0 (o versione successiva) sia installata sul computer virtuale.
La versione non corretta del server ESX è installata sul computer virtuale.	Verificare che la versione del server ESX 4.0 (o versione successiva) sia installata sul computer virtuale.
Spegnimento del sistema server ESX. Lo spegnimento può causare errori durante l'esecuzione dei backup della funzionalità di traccia dei blocchi modificati.	CA ARCserve Central Host-Based VM Backup abilita automaticamente la funzionalità di traccia dei blocchi modificati del computer virtuale.
Riavvio (pulitura) del sistema server ESX mentre il computer virtuale è attivato.	CA ARCserve Central Host-Based VM Backup abilita automaticamente la funzionalità di traccia dei blocchi modificati del computer virtuale.
Il computer virtuale è stato spostato mediante vMotion.	CA ARCserve Central Host-Based VM Backup abilita automaticamente la funzionalità di traccia dei blocchi modificati del computer virtuale.

Backup non riusciti a causa della licenza ESXi

Valido per piattaforme Windows.

Sintomo:

CA ARCserve D2D pieno, incrementale e verificare il processo di backup non riuscito. Viene visualizzato il seguente messaggio nel Registro attività di CA ARCserve D2D:

```
Il server del computer virtuale <server_name> non dispone di una licenza ESX
acquistata.
```

Soluzione:

A causa di una limitazione di VMware, non è possibile eseguire il backup dei computer virtuali in esecuzione sui server ESXi con una licenza gratuita. Per proteggere questi computer virtuali, applicare una licenza acquistata.

Errore di backup e di registrazione dell'evento 1530 nel Registro eventi del sistema proxy di backup

Valido per piattaforme Windows.

Sintomo:

I processi CA ARCserve Central Host-Based VM Backup producono un errore. L'evento 1530 viene registrato nel registro eventi dell'applicazione nel sistema proxy di backup:

Ambienti/Operazioni da riprodurre:

- Microsoft SQL Server o Microsoft Exchange Server vengono installato sul computer virtuale.
- L'utente esegue l'accesso o è già connesso al server proxy CA ARCserve Central Host-Based VM Backup mediante un account di amministratore o un account membro del gruppo di amministratori.
- Dopo aver avviato il processo di backup, l'utente esegue la disconnessione dal server proxy.
- Si verifica un errore del processo di backup. L'evento 1530 viene registrato nel registro eventi dell'applicazione.

  ```
  Avviso emesso dal servizio del profilo utente Microsoft Windows : Il file del
  Registro di sistema è ancora in uso da altri servizi o applicazioni. Il file verrà
  scaricato ora. Dopo lo scaricamento i servizi o le applicazioni che stanno
  utilizzando il file del Registro di sistema potrebbero non funzionare
  correttamente.
  ```

Causa:

Il servizio profili utente di Windows Server 2008 scarica i profili utenti ogni volta che viene eseguita la disconnessione dal computer. Di conseguenza, gli oggetti COM potrebbero non essere creati, impedendo a CA ARCserve Central Host-Based VM Backup di chiamare i moduli COM.

Soluzione:

Per impedire gli errori del processo di backup, eseguire le seguenti operazioni:

Nota: affinché la soluzione funzioni, devono essere presenti tutti i sintomi elencati precedentemente.

1. Accedere al server proxy di CA ARCserve Central Host-Based VM Backup mediante l'account amministratore o un account appartenente al gruppo Amministratori.
2. Avviare l'utilità Editor Criteri di gruppo locali digitando gpedit.msc nella finestra di dialogo Esegui.
3. In Editor Criteri di gruppo locali, espandere Configurazione computer, Modelli amministrativi, Sistema e Profili utente.
4. Dalla directory Profili utente, fare doppio clic su **Non scaricare automaticamente il Registro di sistema relativo agli utenti al momento della disconnessione** per aprire la finestra di dialogo **corrispondente**.
5. Nella finestra di dialogo **Non scaricare automaticamente il Registro di sistema relativo agli utenti al momento della disconnessione,** fare clic su Abilitato, quindi selezionare OK.

   Nota: il valore DisableForceUnload viene aggiunto al Registro di sistema.
6. Riavviare il server CA ARCserve Central Host-Based VM Backup.

I backup vengono completati mediante la modalità di trasporto NBD quando viene specificata la modalità di trasporto hotadd.

Valido per piattaforme Windows.

Sintomo:

I backup del computer virtuale vengono completati mediante la modalità di trasporto NBD (a pagina 203) sebbene sia stata specificata la modalità di trasporto hotadd (a pagina 203).

Soluzione:

CA ARCserve Central Host-Based VM Backup consente di eseguire il backup di computer virtuali che risiedono su sistemi server ESX. Quando viene eseguito il backup di computer virtuali mediante la modalità di trasporto hotadd, è possibile connettere un massimo di 15 dischi virtuali a ciascun controller SCSI sul server proxy del computer virtuale di CA ARCserve D2D. Se viene inoltrato un backup che include più di 15 dischi virtuali e un solo controller SCSI sul server proxy del computer virtuale di CA ARCserve D2D, il controller SCSI non è in grado di ospitare tutti i computer virtuali. Di conseguenza, CA ARCserve Central Host-Based VM Backup esegue il backup dei dati utilizzando la modalità di trasporto NBD.

Per evitare tale situazione, verificare che il numero di controller SCSI sul server proxy del computer virtuale di CA ARCserve D2D sia sufficiente ad ospitare tutti i computer virtuali del processo di backup.

Processi di backup incrementale elaborati come processi di backup di verifica

Valido per Windows

Sintomo:

Durante l'invio o la pianificazione di processi di backup incrementali mediante la modalità di trasporto Hotadd, si verifica il seguente comportamento:

- I processi incrementali si convertono in processi di verifica di backup. La voce del registro attività per il processo indica che il processo di backup incrementale è stato convertito in un processo di backup di verifica.
- La gestione snapshot del client VI del computer virtuale di cui è stato eseguito il backup contiene una snapshot di aiuto consolidata.
- La finestra di dialogo di modifica delle impostazioni del client VI per il computer virtuale interessato indica la presenza di dischi contenenti errori associati al sistema proxy di backup. Gli URL VMDK associati ai dischi contenenti errori non corrispondo a quelli associati al sistema proxy di backup.

Soluzione:

Per risolvere questo problema, rimuovere i file VMDK con errori (dischi) dal sistema proxy di backup utilizzando le linee guida descritte nell'articolo 1003302 della Knowledge Base di VMware. Inoltre, è consigliabile che il valore dello spazio libero sull'archivio dati corrisponda al doppio della dimensione totale dei file del computer virtuale.

Errore dei processi di backup causati da blocchi non identificati

Valido per Windows

Sintomo:

I processi di backup di computer producono un errore e nel Registro attività viene visualizzato il seguente messaggio:

```
L'applicazione non è in grado di individuare i blocchi utilizzati o modificati sul computer virtuale. Questo problema può verificarsi in caso di riavvio del sistema server ESX durante l'esecuzione del computer virtuale. Alla successiva esecuzione di un processo di backup, l'applicazione reimposterà la funzionalità di traccia dei blocchi modificati ed eseguirà un'operazione del backup di verifica.
```

Soluzione:

Per risolvere il problema, eseguire un'operazione di consolidamento disco sul computer virtuale. Per eseguire il consolidamento del disco, eseguire la seguente procedura.

1. Aprire il client VI di VMware.
2. Espandere il sistema server ESX per il computer virtuale interessato.
3. Fare clic con il tasto destro del mouse sul computer virtuale interessato, selezionare Snapshot, quindi Consolida dal menu di scelta rapida per consolidare i dischi.
4. Inoltrare nuovamente il backup.

Impossibile aprire il file VMDK

Valido per piattaforme Windows.

Sintomo:

Più processi di backup simultanei non hanno esito positivo nella modalità di trasporto NDB (o LAN). Il seguente messaggio viene visualizzato nel Registro attività:

```
Impossibile aprire il file VMDK
```

Soluzione:

Questo è un limite di connessione VMware. I seguenti limiti del protocollo NFC (Network File Copy) si applicano:

- ESX 4: 9 connessioni dirette, massimo
- ESX 4 tramite server vCenter: 27 connessioni, massimo
- ESXi 4: 11 connessioni dirette, massimo
- ESXi 4 tramite server vCenter: 23 connessioni, massimo

Le connessioni non possono essere condivise tra dischi. I valori massimi non sono applicabili a connessioni hot-add o SAN. Se il client NFC non si chiude correttamente, le connessioni possono rimanere aperte per dieci minuti.

I nodi non compaiono nella schermata Nodo dopo la modifica del nome del nodo

Valido per piattaforme Windows.

Sintomo:

Il nome host del nodo è stato modificato dopo l'aggiunta alla schermata Nodo. Il nodo non viene più visualizzato nella schermata Nodo.

Soluzione:

Si tratta di un comportamento normale. CA ARCserve Central Host-Based VM Backup conserva il nome del nodo perché è stato aggiunto dalla schermata Nodo. Quando si rinomina il nodo, l'applicazione non è in grado di rilevare il nodo. Il nodo, pertanto, non viene visualizzato nella schermata Nodo.

Per visualizzare i nodi rinominati nella schermata Nodo, procedere come segue:

1. Rinominare il nodo.
2. Aprire la schermata Nodo ed eliminare il nodo (a pagina 51) rinominato.
3. Aggiungere il nodo utilizzando il nuovo nome.

Errore di connessione multipla durante il salvataggio o l'assegnazione di un criterio a un server CA ARCserve D2D.

Applicabile a tutte le piattaforme Windows.

Sintomo:

Durante il tentativo di salvataggio o a assegnazione di un criterio a un server CA ARCserve D2D, viene visualizzato il messaggio di errore seguente:

```
Convalida della destinazione di backup non riuscita. Le connessioni multiple a un server o ad una risorsa condivisa da parte di uno stesso utente con vari nomi utente non sono consentite. Disconnettere tutte le connessioni precedenti al server o alla risorsa condivisa e riprovare.
```

Soluzione:

Se il messaggio precedente viene visualizzato quando si tenta di eseguire il salvataggio o a l'assegnazione di un criterio a un server CA ARCserve D2D, è possibile procedere come segue per risolvere il problema:

- Specificare il campo Nome utente in formato "nome computer (o dominio)\nomeutente".
- Individuare il server remoto della cartella condivisa ed eliminare tutte le sessioni dal server CA ARCserve Central Applications o dal server CA ARCserve D2D. Per eliminare le sessioni, procedere come segue:
  - Eseguire il comando:

    ```
    net session \\machinename /delete
    ```
  - Disconnettere la sessione nella directory seguente:

    ```
    Compmgmt.msc > Utilità di sistema > Cartelle condivise > Sessioni > Disconnetti sessione
    ```
- Assicurarsi di utilizzare lo stesso nome utente per accedere alla cartella condivisa remota.
- Salvare, quindi effettuare nuovamente la distribuzione del criterio.

Errore di completamento dei processi di backup del computer virtuale quando il server ESX non è accessibile

Valido per piattaforme Windows.

Sintomo:

Errori di backup del computer virtuale. Il seguente messaggio viene visualizzato nel Registro attività:

```
Impossibile creare snapshot del computer virtuale.
```

Soluzione:

I backup del computer virtuale possono riportare errori se vengono eseguiti contemporaneamente vari backup su un solo sistema server ESX. Il problema non si verifica quando i backup vengono eseguiti su più sistemi server ESX. Per eseguire il backup di computer virtuali, CA ARCserve Central Host-Based VM Backup utilizza snapshot dei dati che risiedono sul computer virtuale. Se vengono eseguite contemporaneamente più operazioni snapshot su un solo sistema, il sistema server ESX potrebbe non rispondere. Sebbene ciò si verifichi solo temporaneamente, l'operazione di backup viene interrotta, causando l'errore dell'operazione.

Per evitare errori di backup, utilizzare la soluzione più adatta al proprio ambiente:

- Ridurre il numero di computer virtuali sottoposti simultaneamente a backup. Ad esempio, se si sta eseguendo il backup di otto computer virtuali contemporaneamente, ridurre la quantità a sette computer virtuali, inoltrare nuovamente il backup, quindi analizzarne i risultati. Se necessario, ridurre il numero di computer virtuali fino alla risoluzione degli errori di backup oppure fino a quando il messaggio di errore non verrà rimosso dal registro attività.

  Per ridurre la quantità di computer virtuali presenti in un backup, annullare l'assegnazione dei computer virtuali dal criterio. Per ulteriori informazioni, consultare la sezione Annullamento dell'assegnazione di criteri da computer virtuali.

- Definizione di un numero limite di backup simultanei Tale approccio consente di controllare la quantità di processi di backup eseguibili contemporaneamente nel proprio ambiente. Per ulteriori informazioni, consultare la sezione Definizione di un numero limite di backup simultanei (a pagina 193).

Collegamento Aggiungi nuova scheda non funzionante per Internet Explorer 8, 9 e Chrome.

Valido per Windows

Sintomo:

Quando viene aggiunto un nuovo collegamento alla scheda della barra di navigazione specificando un URL HTTPS, facendo clic sulla nuova scheda verranno visualizzati i seguenti messaggi di errore:

- Internet Explorer 8 e 9:

  `Il contenuto è stato bloccato poiché non è stato firmato da un certificato di protezione valido.`

- Chrome:

  `La pagina Web non è disponibile.`

Soluzione:

Per correggere il problema relativo a Internet Explorer, eseguire le seguenti operazioni:

- Internet Explorer 8:

  Fare clic sulla barra del messaggio e selezionare Visualizza contenuto bloccato.

- Internet Explorer 9:

  Fare clic sul pulsante Mostra il contenuto della Barra messaggi nella parte inferiore della pagina. La pagina viene aggiornata e il collegamento alla scheda aggiunta viene aperto correttamente.

Per risolvere il problema relativo a Chrome, eseguire le seguenti operazioni:

Fase 1 - Esportazione del certificato:

1. Aprire una nuova scheda in Chrome ed immettere l'URL HTTPS.

   Verrà visualizzato il messaggio di avviso "Il certificato di sicurezza del sito non è affidabile!"

2. Dalla barra degli indirizzi, fare clic sul lucchetto contrassegnato con una X.

   Verrà visualizzata una finestra popup contenente il collegamento a Informazioni sul certificato.

3. Fare clic sul collegamento Informazioni sul certificato.

   Verrà visualizzata la finestra di dialogo Certificato.

4. Fare clic sulla scheda Dettagli, quindi selezionare Copia su file per salvare il certificato sul computer locale.

   Viene visualizzata la procedura guidata di esportazione del certificato.

5. Fare clic su Avanti per selezionare il formato desiderato per l'esportazione del file.

   Nota: X.509 binario codificato DER (.CER) è selezionato per impostazione predefinita.

6. Fare clic su Avanti per selezionare un percorso in cui salvare il certificato.
7. Fare clic su Avanti per completare la procedura guidata di esportazione del certificato, quindi fare clic su Fine.

Il certificato viene esportato correttamente.

Fase 2 - Importazione del certificato:

1. Selezionare Opzioni da Personalizza e controlla Google Chrome.

   Verrà visualizzata la finestra di dialogo Opzioni.

2. Selezionare l'opzione Roba da smanettoni, quindi selezionare Gestisci certificati della sezione HTTPS/SSL.

   Viene visualizzata la finestra di dialogo Certificati.

3. Fare clic su Importa.

   Viene visualizzata la procedura guidata di importazione del certificato.

4. Fare clic su Avanti per ricercare il certificato salvato sul computer locale.
5. Fare clic su Avanti per aprire l'Archivio certificati.

   Verrà visualizzata la finestra di dialogo Archivio certificati.

6. Fare clic su Sfoglia per aprire la finestra di dialogo Selezione archivio certificati.

   Viene visualizzata la finestra di dialogo Selezione archivio certificati.

7. Selezionare Autorità di certificazione fonti attendibili dall'elenco di file, quindi fare clic su OK.

   Viene visualizzata la finestra di dialogo Archivio certificati.

8. Fare clic su Avanti per completare la procedura guidata di importazione del certificato, quindi fare clic su Fine.

   Verrà visualizzata una finestra di dialogo di avviso che comunica all'utente che si sta per installare un certificato.

   Fare clic su Sì per accettare i termini.

Il certificato viene importato correttamente.

Collegamento Aggiungi nuova scheda, Feed RSS e commenti relativi al social network non avviati correttamente in Internet Explorer 8 e 9

Valido per Windows

Sintomo:

Per un URL CA ARCserve Central Applications HTTPS:

Quando viene aggiunto un nuovo collegamento alla scheda della barra di navigazione specificando un URL HTTP, facendo clic sulla nuova scheda e sul collegamento Commenti e suggerimenti verranno visualizzati i seguenti messaggi di errore:

```
La navigazione alla pagina Web è stata annullata.
```

Inoltre, i feed RSS non vengono visualizzati.

Nota: il collegamento Commenti e suggerimenti visualizza un messaggio di errore anche se non viene aggiunto il collegamento alla nuova scheda.

Soluzione:

Per risolvere il problema, procedere come segue:

- Internet Explorer 8:

  Dopo aver eseguito l'accesso, viene visualizzato il messaggio di avviso Visualizzare solo le informazioni della pagina Web fornite in modo protetto? Selezionare No per visualizzare il contenuto non protetto della pagina Web.

- Internet Explorer 9:

  Fare clic sul pulsante Mostra tutto il contenuto della barra dei messaggi nella parte inferiore della pagina. La pagina viene aggiornata e il collegamento alla scheda aggiunta viene aperto correttamente.

Impossibile specificare un asterisco o un carattere di sottolineatura come carattere jolly nei campi di filtro utilizzando la tastiera giapponese

Valido per Windows

Sintomo:

A causa di una differenza di codici con le tastiere giapponesi, non è possibile immettere il carattere jolly "*" e altri caratteri speciali, come ad esempio il carattere di sottolineatura "_" nei seguenti campi di filtro:

- Il problema si verifica soltanto con Firefox:
  - Nodo > Aggiungi gruppo - Campo Filtro Nome nodo
  - Criteri > Scheda Assegnazione criterio > Assegnazione e annullamento assegnazione del criterio - Campo Filtro Nome nodo.
  - Ripristina > Esplorazione nodi - Campo Nome nodo
  - Nodo > Aggiungi nodo dall'elenco di rilevamento > Nodi da proteggere - Campo Nome nodo

Soluzione:

Per impedire che si verifichi il problema, aprire un'applicazione di modifica del testo come ad esempio Notepad. Digitare i caratteri speciali (ad esempio "*" e "_") nell'editor di testo. Copiare quindi i caratteri dall'editor di testo nel campo.

Recupero di un computer virtuale con modalità di trasporto diversa da quella specificata

Valido per piattaforme Windows.

Sintomo:

Il recupero del computer virtuale utilizza una modalità di trasporto diversa dalla modalità specificata nella chiave del registro di sistema.

Soluzione:

Questo comportamento influisce su dischi thin. Per risolvere questo problema, attenersi alla procedura seguente:

1. Accedere al sistema proxy di backup CA ARCserve D2D per i computer virtuali.
2. Aprire l'editor del Registro di sistema e cercare la seguente chiave:

   HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA ARCserve D2D\AFRestoreDll
3. Impostare una delle seguenti modalità di trasporto per la chiave del registro di sistema EnforceTransportForRecovery:
   - NBD
   - NBDSSL
4. Inoltrare il processo di recupero per il computer virtuale.

CA ARCserve Central Host-Based VM Backup non riconosce i volumi sui dischi dinamici durante il recupero del computer virtuale su un server Hyper-V o un server ESX alternativo.

Valido per piattaforme Windows.

Sintomo:

L'applicazione non è in grado di riconoscere i volumi sui dischi dinamici durante il processo di recupero del computer virtuale su un server Hyper-V o un server ESX alternativo.

Alcuni dei dischi non sono in linea e i volumi corrispondenti non sono disponibili al riavvio del computer virtuale.

Soluzione:

Per recuperare i volumi, accedere al computer virtuale remoto di standby e impostare i dischi in linea manualmente da diskmgmt.msc.

Il ripristino dei dati genera problemi se il backup dei dati viene eseguito mediante la modalità di trasporto HotAdd per dischi di dimensioni superiori a 2 TB

Sintomo:

Quando viene eseguito il backup dei file VMDK (virtual machine disk) di dimensioni superiori a 2 TB mediante la modalità di trasporto VMware HotAdd, il backup viene eseguito correttamente ma i dati ripristinati sono corrotti.

Soluzione:

A causa di un problema noto di VMware VDDK (Virtual Disk Development Kit), il processo di backup viene eseguito correttamente ma i dati ripristinati sono corrotti. Per risolvere il problema, eseguire una delle seguenti attività:

- Riconfigurare il piano di backup per consentire l'esecuzione del processo di backup su un proxy di backup differente in modo che non venga eseguito con la modalità di trasporto HotAdd.
- Impostare il registro di sistema affinché la modalità di trasporto utilizzata durante il backup non sia HotAdd. È possibile utilizzare SAN o NBD/NBDSSL.

Per ulteriori informazioni su questo problema VMware, consultare la Documentazione VMware http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2068424.

Capitolo 6: Procedura consigliata

Questa sezione contiene i seguenti argomenti:

Esecuzione del ripristino bare metal di un computer virtuale

Il ripristino bare metal è supportato quando un computer virtuale è attivo al momento dell'esecuzione del processo di backup.

Il processo di ripristino bare metal (BMR) consiste nel ripristino di interi sistemi ed include la reinstallazione del sistema operativo e delle applicazioni software nonché il ripristino di dati e impostazioni. Il processo di ripristino bare metal consente di eseguire facilmente il ripristino completo di un computer, incluso in caso di hardware diverso. È possibile eseguire il ripristino bare metal poiché durante il processo di backup a livello di blocco, CA ARCserve D2D non solo acquisisce i dati, ma anche tutte le informazioni relative ai seguenti elementi:

- Sistema operativo
- Applicazioni installate
- Impostazioni di configurazione
- Driver necessari

Le informazioni necessarie per l'esecuzione di una ricostruzione completa di interi sistemi da bare metal vengono sottoposte a backup in una serie di blocchi ed archiviate nella posizione di backup.

CA Support: Modalità di ripristino bare metal

YouTube: Modalità di ripristino bare metal

Per l'esecuzione di un ripristino BMR è necessario disporre

- di uno dei seguenti elementi:
  - Un'immagine ISO di ripristino bare metal masterizzata su un CD/DVD
  - Un'immagine ISO di ripristino bare metal masterizzata su una periferica USB portatile

  Nota: CA ARCserve D2D utilizza un'utilità del kit di avvio per combinare un'immagine WinPE e un'immagine CA ARCserve D2D per la creazione di un'immagine ISO di ripristino bare metal. Tale immagine viene quindi masterizzata su un supporto di avvio. Sarà quindi possibile utilizzare tali supporti di avvio (CD/DVD o periferica USB) per avviare il nuovo sistema del computer e consentire l'avvio del processo di ripristino bare metal. Al fine di garantire che l'immagine salvata corrisponda sempre alla versione più recente, si consiglia di creare una nuova immagine ISO per ogni aggiornamento di CA ARCserve D2D.
- Almeno un backup completo.
- Almeno 1 GB di RAM installato sul computer virtuale e il server di origine di cui si sta eseguendo il recupero.
- Se si desidera eseguire il recupero di computer virtuali VMware su computer virtuali VMware configurati come server fisici, verificare che gli strumenti VMware siano installati sul computer virtuale di destinazione.

Il ripristino dei dischi dinamici viene eseguito solo a livello del disco. Se il backup dei dati avviene su un volume locale che risiede su un disco dinamico, tale disco non potrà essere ripristinato durante il ripristino bare metal. In tal caso, per eseguire il ripristino durante il ripristino bare metal è necessario eseguire una delle attività seguenti e quindi eseguire il ripristino bare meta dal punto di ripristino copiato:

- Eseguire il backup su un volume di un'altra unità.
- Eseguire il backup su una condivisione remota.
- Copiare un punto di ripristino su una destinazione diversa.

Nota: se si esegue il ripristino bare metal con dischi dinamici multipli, il ripristino potrà non riuscire a causa di alcuni errori imprevisti (come errori di avvio, volumi dinamici non riconosciuti, eccetera). Se ciò si verifica, sarà necessario eseguire il ripristino del disco mediante ripristino bare metal quindi, una volta riavviato il computer, sarà possibile ripristinare i volumi dinamici in un ambiente normale.

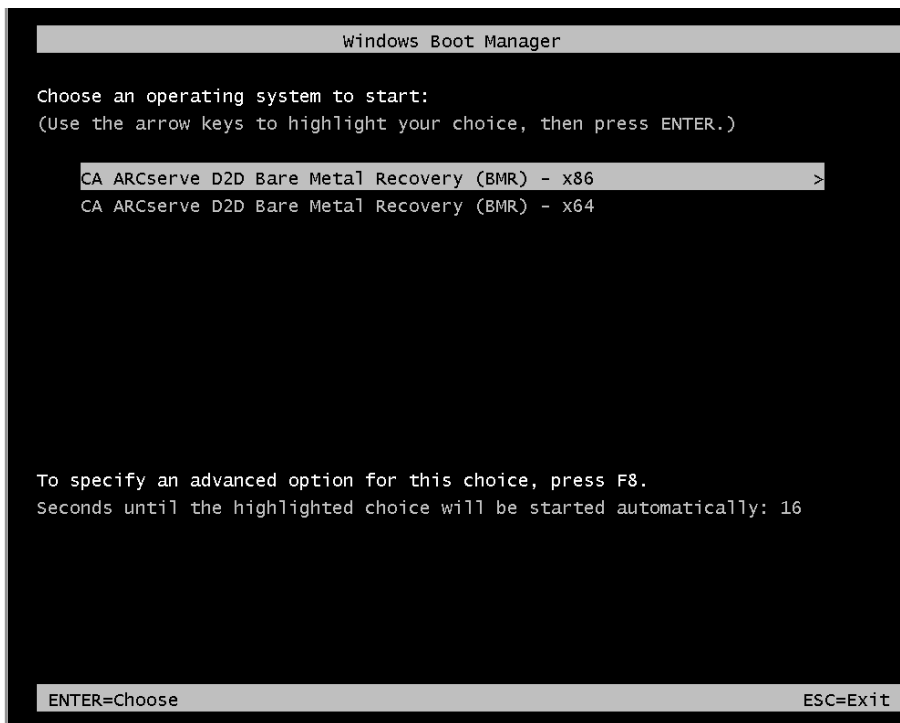
Il processo di ripristino bare metal non cambia, indipendentemente dal metodo utilizzato per la creazione dell'immagine del kit di avvio.

Nota: il processo di ripristino bare metal non è in grado di creare spazi di archiviazione. Se il computer di origine dispone di spazi di archiviazione, durante il ripristino bare metal non sarà possibile creare spazi di archiviazione sul computer di destinazione. È inoltre possibile eseguire il ripristino di tali volumi su dischi o volumi regolari oppure creare manualmente spazi di archiviazione prima dell'esecuzione del ripristino bare metal ed eseguire il ripristino dei dati negli spazi di archiviazione creati.

Per ripristinare i dati mediante ripristino bare metal:

1. Inserire il supporto contenente l'immagine del kit di avvio salvata e avviare il computer.
   - Se si utilizza un'immagine ISO di ripristino bare metal masterizzata su CD/DVD, inserire il CD/DVD salvato.
   - Se si utilizza un'immagine ISO di ripristino bare metal masterizzata su una periferica USB, inserire la periferica USB salvata.

   Verrà visualizzata la schermata dell'utilità di installazione BIOS.

2. In questa schermata, selezionare l'opzione Unità CD-ROM o l'opzione USB per inizializzare il processo di avvio. Selezionare un'architettura (x86/x64) e premere Invio per continuare.

3. Verrà visualizzata la schermata di selezione della lingua di CA ARCserve D2D. Selezionare una lingua e fare clic su Avanti per continuare.

Il processo di ripristino bare metal viene avviato e viene visualizzata la schermata della procedura guidata di ripristino bare metal.

Specificare un tipo di recupero:

◉ **Recupero dei dati di backup mediante CA ARCserve D2D**

(Sessioni di backup eseguite mediante CA ARCserve D2D o CA ARCserve Central Host-Based VM Backup).

○ **Recupero mediante computer virtuale Virtual Standby Hyper-V**

(I dati possono essere ripristinati solo se la conversione virtuale è stata eseguita con CA ARCserve Central Virtual Standby)

○ **Recupero mediante computer virtuale Virtual Standby VMware**

(I dati possono essere ripristinati solo se la conversione virtuale è stata eseguita con CA ARCserve Central Virtual Standby)

4. Dalla schermata della procedura guidata di ripristino bare metal, selezionare il tipo di ripristino bare metal che si desidera eseguire:

   - **Recupero dei dati di backup mediante CA ARCserve D2D**

     Consente di recuperare i dati per cui è stato eseguito il backup mediante CA ARCserve D2D. Questa opzione viene utilizzata nel caso di connessioni di backup eseguite con CA ARCserve D2D oppure con l'applicazione CA ARCserve Central Host-Based VM Backup.

     Se si seleziona questa opzione, continuare questa procedura da questo punto.

   - **Recupero mediante computer virtuale Virtual Standby Hyper-V**

     Consente di eseguire il recupero dei dati per un computer la cui conversione virtuale viene eseguita da un computer virtuale Hyper-V. Questa opzione viene utilizzata per l'applicazione CA ARCserve Central Virtual Standby.

     Nota: l'opzione consente di eseguire il recupero dei dati solo se la conversione virtuale a file VHD (per Hyper-V) è stata eseguita mediante CA ARCserve Central Virtual Standby.

     Se si seleziona questa opzione, consultare la sezione Recupero mediante computer virtuale Virtual Standby Hyper-V per continuare la procedura.

   - **Recupero mediante computer virtuale Virtual Standby VMware**

     Consente di eseguire il recupero dei dati per un computer la cui conversione virtuale viene eseguita da un computer virtuale VMware. Questa opzione viene utilizzata per l'applicazione CA ARCserve Central Virtual Standby.

     Nota: l'opzione consente di eseguire il recupero dei dati solo se la conversione virtuale a file VMDK (per VMware) è stata eseguita mediante CA ARCserve Central Virtual Standby.

     Se si seleziona questa opzione, consultare la sezione Recupero mediante computer virtuale Virtual Standby VMware per continuare la procedura.

5. Fare clic su Avanti.

   Verrà visualizzata la schermata della selezione guidata del punto di ripristino.

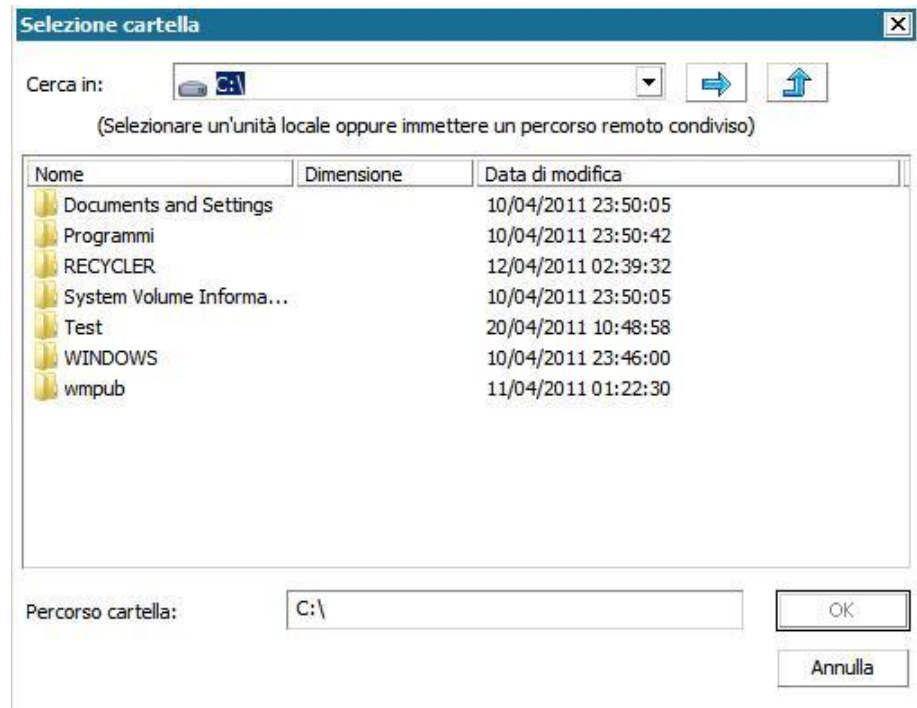
6. Dalla schermata della selezione guidata di un punto di ripristino, selezionare il computer (o il volume) contenente i punti di ripristino per l'immagine di backup.

   CA ARCserve D2D consente di eseguire il recupero da un'unità locale o da una condivisione di rete.

   - Se si esegue il recupero da un backup locale, la procedura guidata di ripristino bare metal individua e visualizza automaticamente tutti i volumi che contengono punti di ripristino.
   - Se si sta eseguendo il recupero da una condivisione remota, individuare la posizione remota di archiviazione dei punti di ripristino. Se i punti di ripristino sono contenuti su più computer, verranno visualizzati tutti i computer.

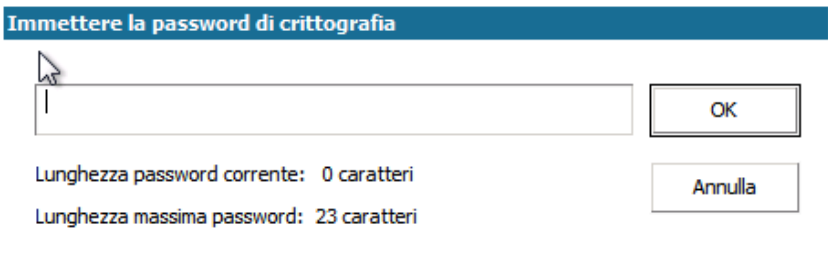
     Potrebbe essere necessario disporre delle informazioni di accesso (nome utente e password) del computer remoto.

     Nota: per poter individuare i punti di ripristino remoti, la rete deve essere attiva e in esecuzione. Se necessario, è possibile verificare o aggiornare le informazioni relative alla configurazione di rete oppure caricare i driver mancanti dal menu Utilità.

7. Se il modulo di ripristino bare metal non è in grado di rilevare i volumi di destinazione locali, viene visualizzata automaticamente la finestra di dialogo Selezionare una cartella. Specificare la condivisione remota su cui risiede il backup..

8. Selezionare la cartella di archiviazione dei punti di ripristino per il backup e fare clic su OK. Per convalidare la connessione alla posizione selezionata, fare clic sull'icona della freccia.

   La schermata della procedura guidata di ripristino bare metal visualizza le informazioni seguenti:

   - Nome computer (riquadro sinistro superiore).
   - Informazioni di backup (riquadro destro superiore).
   - Punti di ripristino corrispondenti (riquadro sinistro inferiore).

   Nota: i sistemi operativi supportati consentono di eseguire un ripristino bare metal a partire a un backup eseguito su un computer UEFI su un computer BIOS e da un computer BIOS su un computer UEFI. Consultare la sezione Sistemi operativi che supportano la conversione UEFI/BIOS per un elenco completo di sistemi supportati per la conversione firmware.

     - Per sistemi operativi che non supportano la conversione firmware, è necessario avviare il computer in modalità UEFI per l'esecuzione di un ripristino bare metal per un sistema UEFI. Il ripristino bare metal non supporta il ripristino di un computer con firmware diverso. Per verificare che il firmware di avvio utilizzato corrisponde a UEFI e non BIOS, fare clic su Utilità e selezionare Informazioni.
     - Per sistemi operativi che supportano la conversione firmware, dopo aver selezionato il punto di ripristino, se il computer di origine non corrisponde al firmware del sistema, verrà richiesto se si desidera convertire il sistema UEFI in un sistema compatibile con BIOS o il sistema BIOS in un sistema compatibile con UEFI.

ARCserve D2D Bare Metal Recovery
Ripristino bare metal (BMR) di CA ARCserve D2D
- Selezionare un punto di ripristino
Il riquadro superiore visualizza tutti i computer di cui è stato eseguito il backup e le relative destinazioni di backup. Facendo clic su un computer, sarà possibile visualizzare nel riquadro inferiore i punti di ripristino associati. Selezionare un punto di ripristino per continuare.
Nota: per impostazione predefinita, vengono elencati solo i computer di cui è stato eseguito il backup e rilevati da volumi locali. Quando viene inserito o rimosso un nuovo disco rimovibile, fare clic su Aggiorna per aggiornare l'elenco dei computer.
Fare clic su Sfoglia per aggiungere i computer di cui è stato eseguito il backup dalla cartella remota condivisa.
Se la cartella remota condivisa non può essere individuata, potrebbe trattarsi di un problema di installazione del driver NIC oppure di validità
Rilevate 1 schede di rete
Intel(R) PRO/1000 MT Network Connection
- Indirizzo IP: 155.35.128.87
- Stato: Connesso
È stato rilevato il backup dei seguenti computer:
Informazioni di backup
Nome host:
Sistema operativo:
Windows 7
Piattaforma:
X64
Aggiorna
Sfoglia
Sono stati rilevati i seguenti punti di ripristino per il computer specificato. Selezionare un punto di ripristino e
17/04/2012
05:42:52
16/04/2012
21:41:44
20:34:22
11/04/2012
Tipo di backup:
- Backup di verifica
Destinazione di backup (rilevata dal sistema corr
- D:\d2d-dest\W2K8R2Ivpef1\
Descrizione backup:
- Backup di verifica personalizzato
Firmware di avvio:
- UEFI
Ripristino bare metal in posizione originale di CA
Utilità
Indietro
Avanti
Interrompi

9. Selezionare il punto di ripristino da ripristinare.

   Vengono visualizzate le informazioni relative al punto di ripristino selezionato (riquadro destro inferiore). La visualizzazione include informazioni quali il tipo di backup eseguito (e salvato), la destinazione di backup e i volumi di cui è stato eseguito il backup.

   Se il punto di ripristino contiene sessioni crittografate, l'icona del punto di ripristino con forma di orologio presenta un lucchetto e viene visualizzata una schermata per l'immissione della password. Immettere la password di sessione, quindi fare clic su OK.

   Nota: se il computer in uso è un controller di dominio, CA ARCserve D2D supporta il ripristino non autorevole del file di database AD (Active Directory) durante il ripristino bare metal. CA ARCserve D2D non supporta il ripristino di cluster MSCS.

10. Verificare che il punto di ripristino selezionato sia corretto, quindi selezionare Avanti.

    Verrà visualizzata la scherma della procedura guidata di ripristino bare metal e le opzioni della modalità di recupero.

11. Selezionare la modalità di recupero.

    Le opzioni disponibili sono Modalità avanzata e Modalità rapida.

    - Selezionare Modalità avanzata per personalizzare il processo di recupero.
    - Selezionare Modalità rapida se si desidera intervenire in modo limitato nel processo di recupero.

    Impostazione predefinita: Modalità rapida.

    Nota: la procedura riportata di seguito descrive le operazioni necessarie per il completamento del processo di ripristino bare metal e sono applicabili solo nel caso in cui sia stata selezionata la Modalità avanzata.

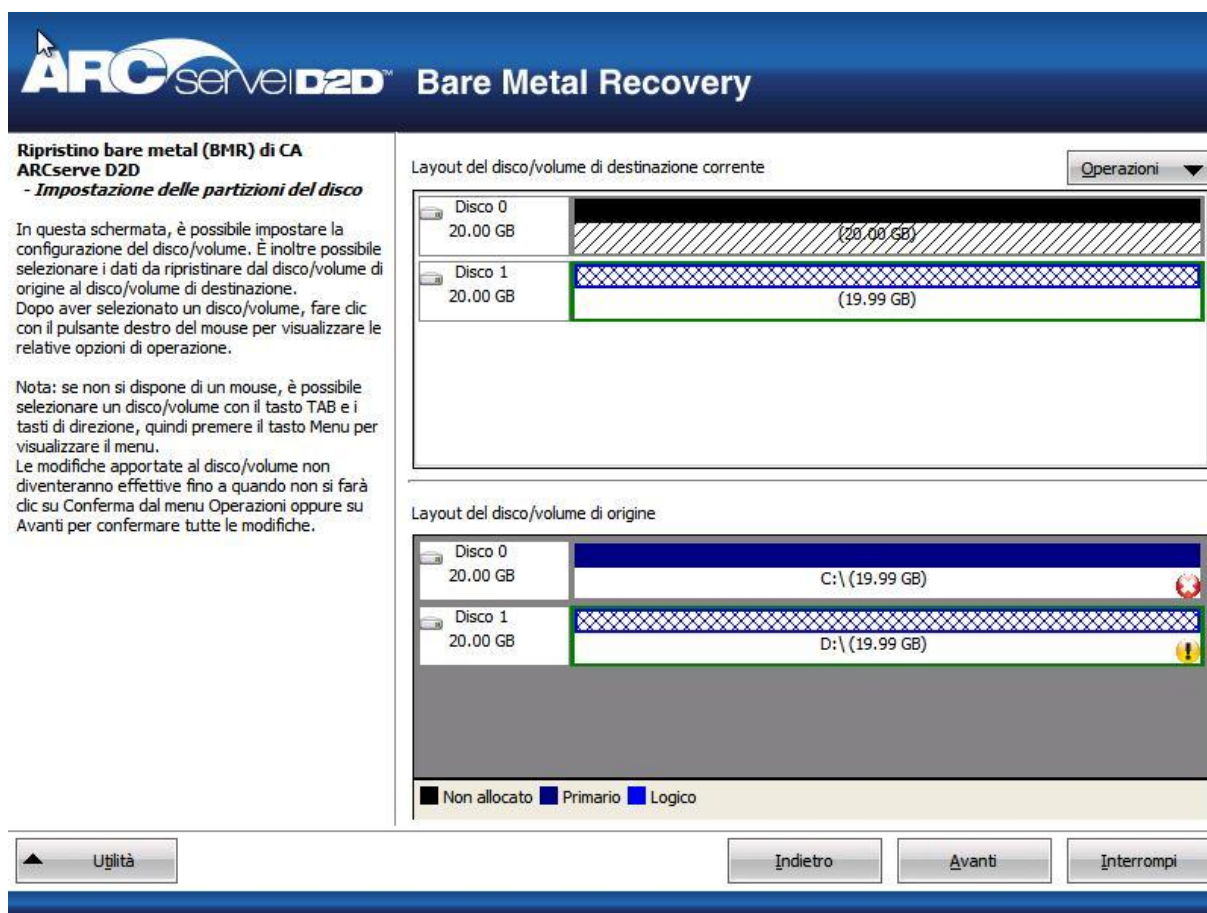
12. Fare clic su Avanti.

    L'utilità di ripristino bare metal esegue la ricerca del computer da recuperare e visualizza le informazioni relative alla partizione del disco corrispondente.

    Il riquadro superiore mostra la configurazione del disco presente sul computer corrente (destinazione), mentre il riquadro inferiore mostra le informazioni relative alla partizione del disco del computer originale (origine).

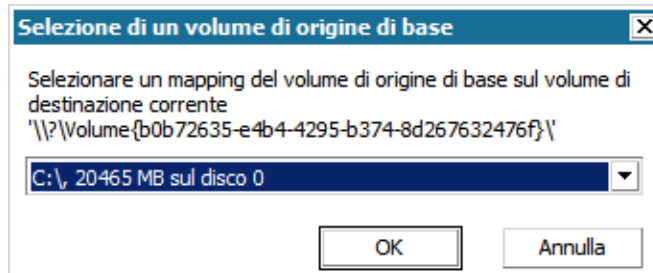
Importante. Se nel riquadro inferiore il volume di origine viene contrassegnato da una X rossa, significa che tale volume contiene informazioni di sistema e che non è stato assegnato (mappato) al volume di destinazione. Il volume contenente le informazioni di sistema dovrà essere assegnato dal disco di origine al disco di destinazione e ripristinato durante il processo di ripristino bare metal. In caso contrario, non sarà possibile eseguire il riavvio.

Nota: se si esegue il ripristino bare metal del volume di sistema su un disco non configurato come disco di avvio, non sarà possibile avviare il computer in seguito al completamento del ripristino bare metal. Assicurarsi di eseguire il ripristino del volume di sistema su un disco di avvio configurato correttamente.

Nota: se si esegue il ripristino su un altro disco/volume, la capacità del nuovo disco/volume deve essere uguale o superiore a quella del disco/volume originale. Inoltre, il ridimensionamento del disco è disponibile solo per i dischi di base e non per i dischi dinamici.

13. Se le informazioni del disco non vengono visualizzate correttamente, accedere al menu Utilità e verificare se sono richiesti driver mancanti.

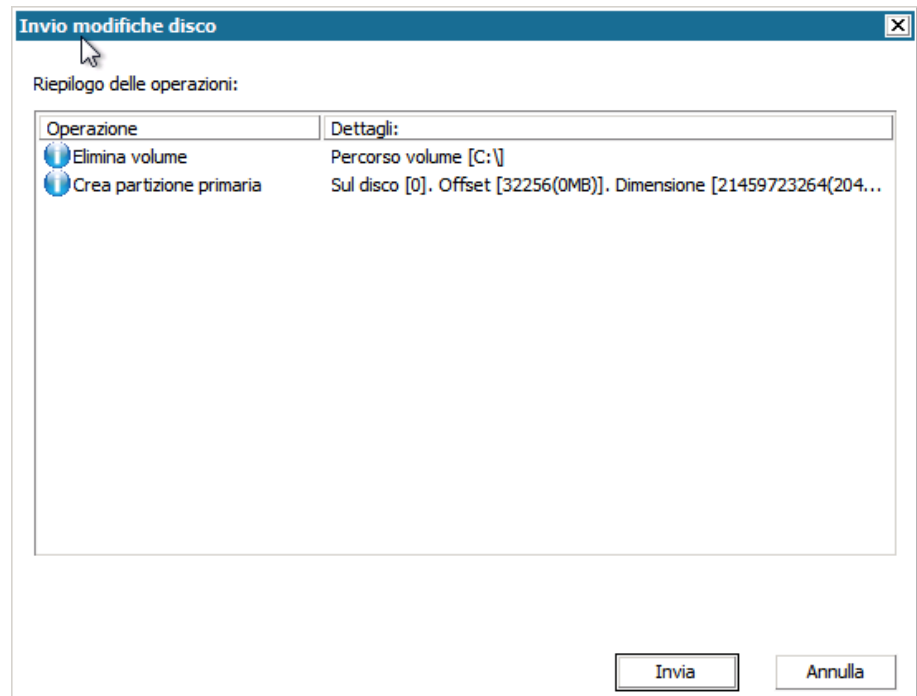
14. Se necessario, nel riquadro del disco/volume di destinazione, è possibile fare clic sul menu a discesa Operazioni e visualizzare le opzioni disponibili. Per ulteriori informazioni sulle opzioni, consultare la sezione Gestione del menu delle operazioni di ripristino bare metal.

15. Per assegnare un volume di origine al volume di destinazione, fare clic su ciascun volume di destinazione e, dal menu di scelta rapida, selezionare l'opzione Esegui mapping del volume da.

    Verrà visualizzata la finestra di dialogo Selezione di un volume di origine di base.

16. Nella finestra di dialogo Selezione di un volume di origine di base, fare clic sul menu a discesa e selezionare il volume di origine disponibile da assegnare al volume di destinazione specificato. Fare clic su OK.

    - Il volume di destinazione viene contrassegnato da un'icona con il segno di spunta, a indicare che il mapping del volume di destinazione è stato eseguito.
    - Nel volume di origine, l'icona con forma di X rossa viene sostituita da un'icona verde, a indicare che il volume di origine è stato assegnato a un volume di destinazione.

17. Verificare che tutti i volumi da ripristinare e che i volumi contenenti informazioni di sistema siano assegnati a un volume di destinazione, quindi fare clic su Avanti.

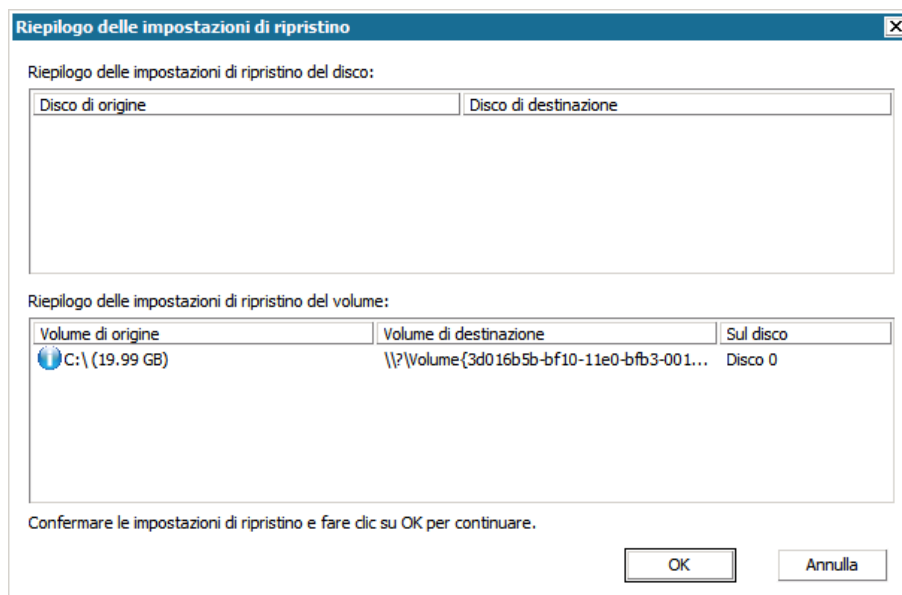
    Verrà visualizzata la schermata Invio modifiche disco contenente un riepilogo delle operazioni selezionate. Per ciascun nuovo volume creato, vengono visualizzate le informazioni corrispondenti.

18. Verificare che le informazioni di riepilogo siano corrette, quindi fare clic su Invia. Se le informazioni non sono corrette, fare clic su Annulla.

    Nota: tutte le operazioni eseguite sul disco rigido verranno implementate solo in seguito all'invio.

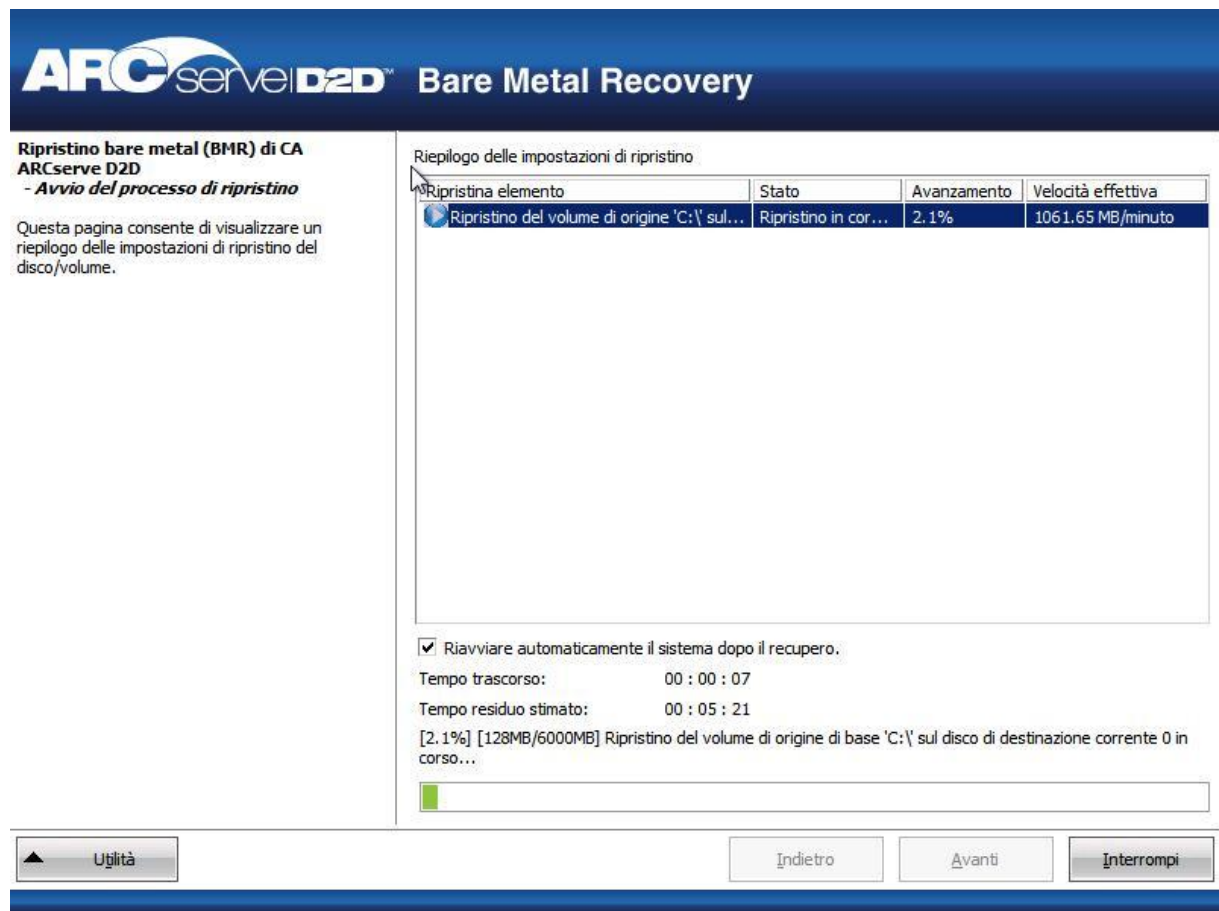
    I nuovi volumi vengono creati sul computer di destinazione e mappati sul computer di origine corrispondente.

19. Una volta completate le modifiche, fare clic su OK.

    Verrà visualizzata la schermata Riepilogo delle impostazioni di ripristino contenente un riepilogo dei volumi da ripristinare.

    Nota: nella parte superiore della pagina Riepilogo di ripristino, le lettere corrispondenti alle unità elencate nella colonna Volume di destinazione vengono generate automaticamente dall'Ambiente di preinstallazione di Windows (WinPE). È possibile che tali lettere di unità non corrispondano alle lettere elencate nella colonna Volume di origine. Tuttavia, il ripristino dei dati verrà eseguito sul volume appropriato anche se le lettere di unità sono diverse.

20. Verificare che le informazioni di riepilogo siano corrette, quindi fare clic su OK.

    Verrà avviato il processo di ripristino. La schermata della procedura guidata di ripristino bare metal visualizza lo stato di ripristino per ciascun volume.

    - Il tempo necessario per l'esecuzione di questa operazione dipende dalle dimensioni del volume da ripristinare.
    - Durante questo processo viene eseguito il ripristino blocco per blocco di tutti i dati di backup di tale punto di ripristino e viene creata una replica del computer di origine sul computer di destinazione.
    - L'opzione di riavvio automatico del sistema in seguito al recupero è selezionata per impostazione predefinita. Se lo si desidera, è possibile deselezionare questa opzione ed eseguire il riavvio manuale in un secondo momento.
    - Se necessario, è possibile annullare o interrompere l'operazione in qualsiasi momento.

21. Dal menu Utilità, è possibile accedere al registro attività del ripristino bare metal e utilizzare l'opzione Salva per salvare il registro attività.

    Per impostazione predefinita, il salvataggio del registro attività viene effettuato nella posizione seguente:

    X:\windows\system32\dr\log.

    Nota: per evitare la generazione di un errore Windows, si consiglia di non utilizzare l'opzione Salva con nome della finestra di dialogo del registro attività del ripristino bare metal per salvare il registro attività sul desktop o per creare una nuova cartella sul desktop.

22. Se si sta eseguendo il ripristino su hardware diversi (la scheda SCSI/FC utilizzata per la connessione ai dischi rigidi potrebbe essere stata modificata) e non viene rilevato nessun driver compatibile nel sistema originale, viene visualizzata la pagina di inserimento del driver per consentire all'utente di specificare i driver necessari per le periferiche.

    È possibile individuare e selezionare i driver da inserire nel sistema ripristinato. In tal modo è possibile eseguire il ripristino su un computer con hardware diversi.

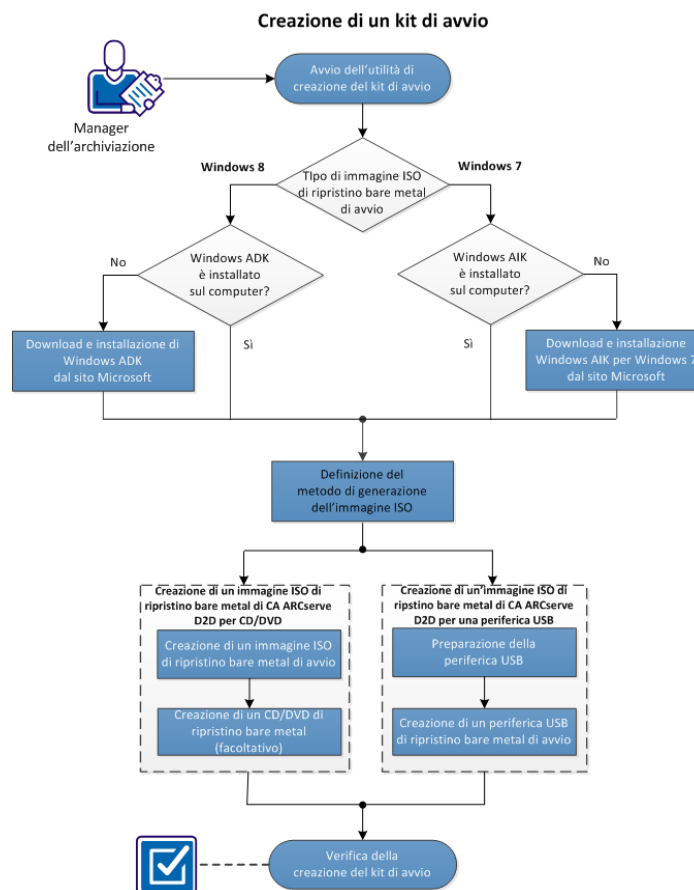
23. Una volta completato il processo di ripristino bare metal, viene visualizzata una notifica di conferma.

Nota: una volta completato il ripristino bare metal:

- Verrà eseguito per primo il backup di verifica.
- Verificare che la BIOS sia configurata per l'avvio dal disco utilizzato per il ripristino del volume di avvio.
- Dopo aver riavviato il computer, potrebbe essere necessario configurare manualmente le schede di rete, nel caso in cui sia stato eseguito il ripristino su hardware differenti.
- Durante il riavvio di un computer, potrebbe essere visualizzata la schermata Ripristino da errori di Windows indicante che l'arresto di Windows non è avvenuto correttamente. Se ciò si verifica, è possibile ignorare l'avviso e avviare Windows normalmente.
- In caso di dischi dinamici, se il disco è in modalità Non in linea, è possibile modificare manualmente lo stato a In linea, accedendo all'interfaccia di gestione del disco mediante l'utilità di controllo Diskmgmt.msc.
- In caso di dischi dinamici, se lo stato del volume è Ridondanza non riuscita, è possibile eseguire la sincronizzazione manuale dei volumi, accedendo all'interfaccia di gestione del disco mediante l'utilità di controllo Diskmgmt.msc.

Creazione di un kit di avvio

CA ARCserve D2D utilizza un'utilità del kit di avvio per combinare un'immagine WinPE e un'immagine CA ARCserve D2D per la creazione di un'immagine ISO di ripristino bare metal. Tale immagine viene quindi masterizzata su un supporto di avvio. Quando si esegue un ripristino bare metal, il disco di avvio di CA ARCserve D2D (CD/DVD o periferica USB) consente l'avvio del nuovo sistema e del processo di ripristino bare metal.

Il diagramma seguente mostra il processo di creazione di un punto di ripristino:

Per creare un kit di avvio, attenersi alla procedura riportata di seguito:

1. Avvio dell'utilità di creazione del kit di avvio (a pagina 182)
2. Definizione del metodo di generazione dell'immagine ISO di ripristino bare metal (a pagina 185)
3. Creazione di un'immagine ISO di ripristino bare metal CA ARCserve D2D per un CD/DVD (a pagina 186)
    a. Crea immagine ISO di ripristino bare metal di avvio (a pagina 186)
    b. (Facoltativo) Creazione di un CD/DVD di ripristino bare metal (a pagina 189)
4. Creazione di un'immagine ISO di ripristino bare metal CA ARCserve D2D per una periferica USB (a pagina 189)
    a. Preparazione di una periferica USB (a pagina 190)
    b. Crea periferica USB di ripristino bare metal di avvio (a pagina 191)
5. Verifica della creazione del kit di avvio (a pagina 193)

VIDEO SUPPLEMENTARE

Questa procedura contiene un video informativo aggiuntivo. Selezionare o CA Support o YouTube come origine di visualizzazione del video. L'unica differenza tra le versioni dei video disponibili su CA Support e YouTube consiste nell'origine di visualizzazione.

CA Support: Creazione di un kit di avvio

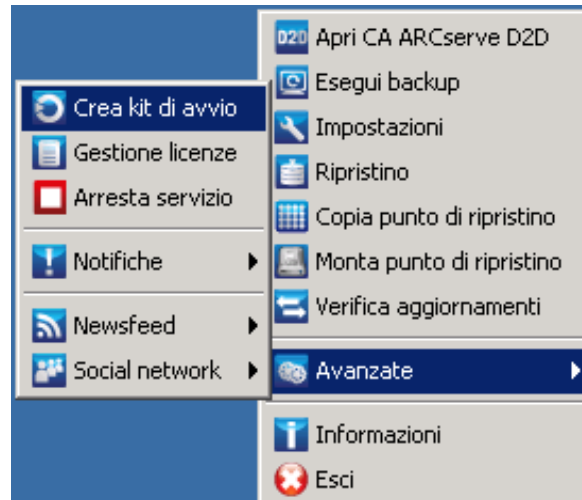
YouTube: Creazione di un kit di avvio

Avvio dell'utilità di creazione del kit di avvio

CA ARCserve D2D fornisce la creazione di un kit di avvio per l'utilità di ripristino bare metal. In tal modo è possibile generare un'immagine ISO basata su WinPE. L'immagine ISO contiene tutte le informazioni necessarie per l'esecuzione di un ripristino bare metal (se necessario).

Procedere come descritto di seguito:

1. È possibile avviare l'utilità Crea kit di avvio dalle opzioni Avanzate del monitoraggio della barra delle applicazioni oppure dal menu Start.

   L'utilità di creazione del kit di avvio viene avviata e viene visualizzata la schermata Definizione del tipo di immagine ISO di ripristino bare metal.

2. Specificare il tipo di immagine ISO di ripristino bare metal da creare (Windows 8 o Windows 7), quindi fare clic su Avanti.

   Nota: Windows XP, Windows Vista e Windows Server 2003 non sono supportati per la creazione di un'immagine ISO di ripristino bare metal. Per questi sistemi operativi, è possibile utilizzare Windows Vista SP1, Windows 2003 SP2 o una versione successiva di Windows.

   - **Windows 8**

     Quando viene avviata, l'utilità esegue immediatamente verifiche sul computer per stabilire se Windows Assessment and Deployment Kit (ADK) è già stato installato. Windows ADK è uno strumento di Microsoft che consente di distribuire i sistemi operativi Windows sui computer.

     Nota:è possibile installare Windows ADK sui computer in esecuzione sui seguenti sistemi operativi:

     – Windows 7

     – Windows Server 2008

     – Windows Server 2008 R2

     – Windows 8

     – Windows Server 2012

   - **Windows 7**

Quando viene avviata, l'utilità esegue immediatamente verifiche sul computer per stabilire se Windows Installation Kit (AIK) è già stato installato. Windows AIK è uno strumento di Microsoft che consente di distribuire i sistemi operativi Windows sui computer.

Nota:è possibile installare Windows AIK per Windows 7 sui computer in esecuzione sui seguenti sistemi operativi:

- Windows 2003 SP2
- Windows Vista SP1
- Windows 7
- Windows Server 2008
- Windows Server 2008 R2

3. Per creare l'immagine ISO di avvio, è necessario che Windows ADK o AIK sia installato sul computer.

   a. Se Windows ADK (o AIK) viene installato, l'utilità avanzerà alla schermata Selezione del metodo del kit di avvio per consentire la creazione del kit di avvio.

   b. Se Windows ADK (o AIK) non viene installato, la schermata Informazioni di Windows corrispondente verrà visualizzata. È necessario scaricare e installare Windows ADK (o AIK) dall'Area download Microsoft.

   Nota: per ulteriori informazioni sull'installazione di Windows ADK (o AIK), consultare i siti Web seguenti:

   - Installazione di Windows ADK
   - Installazione di Windows AIK per Windows 7

   È possibile installare Windows ADK (o AIK) mediante uno dei due metodi seguenti:

   - Scaricare i supporti di installazione direttamente dal sito Web di Microsoft e installare Windows ADK (o AIK) sul proprio computer.
   - Selezionare i collegamenti della schermata informativa per aprire il sito Web di Microsoft, scaricare Windows ADK (o AIK) e installarlo sul proprio computer.

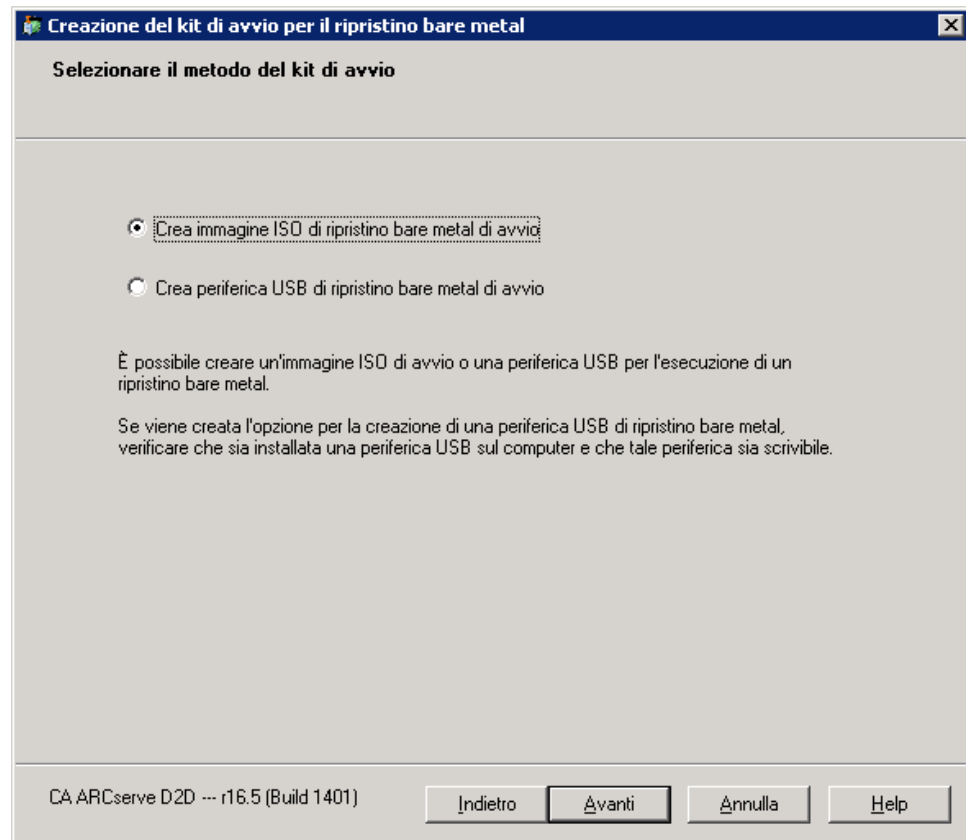
     Dopo avere installato Windows ADK (o AIK), fare clic su Avanti. L'utilità accederà alla schermata Selezione del metodo del kit di avvio per procedere con la creazione del kit di avvio.

   Nota: per l'installazione di Windows ADK, dovranno essere soddisfatte le seguenti funzionalità per la creazione del kit di avvio:

   - Strumenti di distribuzione
   - Ambiente di pre-installazione di Windows (Windows PE)

   Nota: per l'installazione di Windows AIK, selezionare Installazione di Windows AIK.

Definizione del metodo di generazione dell'immagine ISO di ripristino bare metal

L'utilità di creazione del kit di avvio fornisce due opzioni per la generazione di un'immagine ISO:

- Crea immagine ISO di ripristino bare metal di avvio (a pagina 186)

  Questo metodo consente di creare un'immagine ISO masterizzabile su un CD/DVD per l'archiviazione. Questa è l'opzione predefinita. Per ulteriori informazioni, consultare la sezione Creazione di un'immagine ISO di ripristino bare metal CA ARCserve D2D per un CD/DVD (a pagina 186).

- Crea periferica USB di ripristino bare metal di avvio (a pagina 191)

  Questo metodo crea un'immagine ISO e la masterizza direttamente su una periferica USB per l'archiviazione. Per ulteriori informazioni, consultare la sezione Creazione di un'immagine ISO di ripristino bare metal CA ARCserve D2D per una periferica USB (a pagina 189).

Sarà quindi possibile utilizzare tali supporti di avvio per avviare il nuovo sistema del computer e consentire l'avvio del processo di ripristino bare metal. Al fine di garantire che l'immagine salvata corrisponda sempre alla versione più recente, si consiglia di creare una nuova immagine ISO per ogni aggiornamento di CA ARCserve D2D.

Nota: se si esegue un ripristino bare metal su un computer virtuale, è possibile associare direttamente l'immagine ISO al computer virtuale per avviare il processo di ripristino bare metal senza necessità di masterizzarlo su un CD/DVD.

Creazione di un'immagine ISO di ripristino bare metal CA ARCserve D2D per un CD/DVD

Il processo per la creazione di un'immagine ISO di ripristino bare metal di CA ARCserve D2D consiste in:

- Crea immagine ISO di ripristino bare metal di avvio (a pagina 186)
- Creazione di un CD/DVD di ripristino bare metal (a pagina 189)

Crea immagine ISO di ripristino bare metal di avvio

Se si desidera creare un'immagine ISO di ripristino bare metal, è possibile masterizzare l'immagine su un supporto di avvio (CD o DVD) per l'avvio del sistema del computer e consentire l'avvio del processo di ripristino bare metal.

Procedere come descritto di seguito:

1. Dalla schermata Selezione del metodo del kit di avvio, selezionare Crea immagine ISO di ripristino bare metal di avvio, quindi fare clic su Avanti.

   Viene visualizzata la finestra di dialogo Selezione di una piattaforma e di una destinazione.

2. Selezionare la piattaforma adatta per l'immagine ISO.

   È possibile selezionare una delle opzioni disponibili oppure entrambe. Se vengono selezionate entrambe le piattaforme, la creazione dell'immagine richiederà più tempo.

   Nota: un'immagine ISO creata da una piattaforma a 32 bit può essere utilizzata per il ripristino di server a 32 bit. Un'immagine ISO creata da una piattaforma a 64 bit può essere utilizzata per il ripristino di server a 64 bit. Se si desidera avviare un sistema firmware UEFI, verificare che sia selezionata l'opzione per piattaforme x64.

   Le opzioni disponibili sono:

   - Immagine ISO di ripristino bare metal solo per piattaforme x86.
   - Immagine ISO di ripristino bare metal solo per piattaforme x64.
   - Immagine ISO di ripristino bare metal per piattaforme x86 e x64.

3. Specificare la destinazione.

   Specificare o accedere alla posizione in cui verrà creato e archiviato il file dell'immagine ISO di ripristino bare metal.

4. Specificare il nome del file di immagine ISO di ripristino bare metal generato.
5. Dopo avere specificato la piattaforma e la destinazione, fare clic su Avanti.

   Verrà visualizzata la finestra di dialogo Seleziona lingue.

6. Selezionare la lingua per l'immagine ISO di ripristino bare metal generata. Durante la procedura di ripristino bare metal, l'interfaccia utente e la tastiera vengono integrate con la lingua selezionata.

   È possibile selezionare uno o più lingue per l'immagine ISO di ripristino bare metal. Tuttavia, per ogni lingua selezionata, il tempo di creazione dell'immagine sarà superiore. Quante più lingue si selezionano, tanto più lungo sarà il tempo richiesto per il completamento. Si consiglia pertanto di selezionare soltanto le lingue necessarie.

7. Fare clic su Avanti.

   Verrà visualizzata la finestra di dialogo Specificazione dei driver.

8. Specificare i driver che si desidera integrare all'immagine ISO di ripristino bare metal per aggiungerli all'elenco dei driver.

   Il riquadro dei driver viene abilitato ed è possibile specificare qualsiasi driver aggiuntivo che si desidera aggiungere (o eliminare) dall'immagine ISO di ripristino bare metal.

   Nota: quando si esegue l'integrazione del driver di scheda VirtualBox Host-Only Ethernet con un'immagine ISO di ripristino bare metal, è possibile che si verifichi un conflitto con i componenti Windows ADK. Per evitare qualsiasi conflitto, si consiglia di non integrare il driver nell'immagine ISO di ripristino bare metal.

   a. Includi driver locali: consente di caricare i driver di periferiche critiche locali (soltanto i driver oem per NIC, FC o SCSI) nell'elenco dei driver. Dopo essere stata selezionata, l'utilità esegue verifiche sul computer per stabilire se esistono driver di periferiche da aggiungere all'immagine ISO di ripristino bare metal. Se vengono rilevati driver di periferica critici, tali driver verranno aggiunti automaticamente all'elenco.

   b. Aggiungi driver: consente di accedere ai driver che si desidera aggiungere all'elenco dei driver.

   c. Elimina driver: consente di rimuovere qualsiasi driver selezionato dall'elenco che non si desidera aggiungere all'immagine ISO di ripristino bare metal.

9. Fare clic su Crea per avviare il processo e creare un'immagine ISO di ripristino bare metal di avvio.

   Durante il processo, viene visualizzato lo stato.

10. Al completamento del processo, viene visualizzata una schermata di conferma indicante la corretta generazione dell'immagine ISO di ripristino bare metal. La schermata contiene inoltre la posizione e la piattaforma dell'immagine, oltre al collegamento per l'accesso a tale posizione.

Creazione di un CD/DVD di ripristino bare metal

Dopo la creazione e il salvataggio dell'immagine ISO sulla destinazione specificata, è necessario masterizzare l'immagine su un CD o un DVD di avvio. Sarà quindi possibile utilizzare tali supporti di avvio per avviare il nuovo sistema del computer e consentire l'avvio del processo di ripristino bare metal.

Verificare che l'immagine ISO salvata corrisponda alla versione più recente:

- Si consiglia di creare una nuova immagine ISO per ogni aggiornamento di CA ARCserve D2D.
- Se l'immagine ISO viene salvata su una posizione remota, sarà necessario masterizzare il CD/DVD soltanto se è richiesta l'esecuzione di un ripristino bare metal.
- Se CA ARCserve D2D è installato su più computer, è necessario creare una nuova immagine ISO (ed il CD/DVD corrispondente) da un computer attendibile prima dell'esecuzione del ripristino bare metal. In tal modo l'immagine conterrà tutti gli aggiornamento di CA ARCserve D2D più recenti.

Creazione di un'immagine ISO di ripristino bare metal CA ARCserve D2D per una periferica USB

Il processo per la creazione di una periferica USB di ripristino bare metal di CA ARCserve D2D consiste in:

Preparazione di una periferica USB (a pagina 190)

Crea periferica USB di ripristino bare metal di avvio (a pagina 191)

Preparazione di una periferica USB

Prima di masterizzare l'immagine ISO di ripristino bare metal su una periferica USB, è necessario preparare tale periferica. Per la creazione di una periferica USB di ripristino bare metal di avvio, è necessario attivare la periferica per consentire l'avvio del sistema. Per abilitare la periferica, è possibile utilizzare il comando DiskPart.

Importante. Se è necessario formattare la periferica USB, il processo eliminerà tutti i dati archiviati sulla periferica USB. Prima di eseguire il processo, verificare che la periferica non contenga file importanti. Se la periferica USB è stata formattata precedentemente, il processo sovrascriverà tutti i file con lo stesso nome.

Procedere come descritto di seguito:

1. Aprire un prompt dei comandi (con diritti di amministrazione se richiesto dal proprio sistema operativo).
2. Digitare **Diskpart** e premere Invio.
3. Digitare **List Disk** e premere Invio.

   Viene visualizzato un elenco di tutti i dischi rilevati. Determinare tra l'elenco dei dischi rilevati quale sia il proprio.
4. Selezionare il disco USB digitando **Select Disk <n> ("n" corrisponde al numero di disco per il disco USB),** quindi premere Invio.
5. Digitare **Clean** e premere Invio.

   Il sistema visualizzerà il seguente messaggio: "DiskPart succeeded in cleaning the disk."
6. Digitare **create partition primary** e premere Invio.

   Il sistema visualizzerà il seguente messaggio: "succeeded in creating the specified partition".
7. Digitare **select partition 1** e premere Invio.

   Il sistema visualizzerà il seguente messaggio: Partition 1 is now the selected partition.
8. Digitare **active** e premere Invio.

   Il sistema visualizzerà il seguente messaggio: "DiskPart marked the current partition as active."
9. Se necessario, formattare la periferica USB con file system FAT32 o NTFS.

   Digitare **format fs=fat32 quick** oppure **format fs=ntfs quick**

La periferica USB è pronta per l'uso.

Crea periferica USB di ripristino bare metal di avvio

Se si seleziona la creazione di una periferica USB di ripristino bare metal di avvio, è possibile masterizzare l'immagine ISO direttamente su una periferica USB per avviare il nuovo sistema del computer e consentire l'avvio del processo di ripristino bare metal.

Procedere come descritto di seguito:

1. Se necessario, preparare la periferica USB. Per ulteriori informazioni, consultare la sezione Preparazione di una periferica USB (a pagina 190).
2. Dalla schermata Selezione del metodo del kit di avvio, selezionare Crea periferica USB di ripristino bare metal di avvio, quindi fare clic su Avanti.

   Viene visualizzata la finestra di dialogo Selezione di una piattaforma e di una destinazione.

3. Selezionare la piattaforma adatta per l'immagine ISO.

   È possibile selezionare una delle opzioni disponibili oppure entrambe. Se vengono selezionate entrambe le piattaforme, la creazione dell'immagine richiederà più tempo.

   Nota: un'immagine ISO creata da una piattaforma a 32 bit può essere utilizzata per il ripristino di server a 32 bit. Un'immagine ISO creata da una piattaforma a 64 bit può essere utilizzata per il ripristino di server a 64 bit. Se si desidera avviare un sistema firmware UEFI, verificare che sia selezionata l'opzione per piattaforme x64.

   Le opzioni disponibili sono:

   - Immagine ISO di ripristino bare metal solo per piattaforme x86.
   - Immagine ISO di ripristino bare metal solo per piattaforme x64.
   - Immagine ISO di ripristino bare metal per piattaforme x86 e x64.

4. Specificare la periferica USB.

   Specificare o accedere alla posizione dell'unità in cui l'immagine ISO di ripristino bare metal verrà creata e masterizzata sulla periferica USB.

   Nota: per un'unità USB, se si desidera avviare il sistema firmware UEFI, sarà necessario formattare l'unità USB come file system FAT32.

5. Verificare che la periferica USB preparata venga inserita nell'unità specificata.
6. Dopo avere specificato la piattaforma e la posizione, fare clic su Avanti.

   Verrà visualizzata la finestra di dialogo Seleziona lingue.

7. Selezionare la lingua per l'immagine ISO di ripristino bare metal generata. Durante la procedura di ripristino bare metal, l'interfaccia utente e la tastiera vengono integrate con la lingua selezionata.

   È possibile selezionare uno o più lingue per l'immagine ISO di ripristino bare metal. Tuttavia, per ogni lingua selezionata, il tempo di creazione dell'immagine sarà superiore. Quante più lingue si selezionano, tanto più lungo sarà il tempo richiesto per il completamento. Si consiglia pertanto di selezionare soltanto le lingue necessarie.

8. Fare clic su Avanti.

   Verrà visualizzata la finestra di dialogo Specificazione dei driver.

9. Se necessario, selezionare l'opzione di integrazione di driver aggiuntivi.

   Il riquadro dei driver viene abilitato ed è possibile specificare qualsiasi driver aggiuntivo che si desidera aggiungere (o eliminare) dall'immagine ISO di ripristino bare metal.

10. Fare clic su Crea per avviare il processo e creare un'immagine ISO di ripristino bare metal di avvio.

    Durante il processo, viene visualizzato lo stato.

11. Al completamento del processo, verrà visualizzata una schermata di conferma indicante che l'immagine ISO di ripristino bare metal è stata generata correttamente e masterizzata sulla periferica USB. La schermata contiene inoltre la posizione e la piattaforma dell'immagine, oltre al collegamento per l'accesso a tale posizione.

Verifica della creazione del kit di avvio

Al completamento del processo di creazione dell'immagine ISO di ripristino bare metal, l'utilità di creazione del kit di avvio mostrerà un collegamento per la connessione alla posizione in cui è stata salvata l'immagine. Verificare che l'immagine ISO di ripristino bare metal sia stata salvata nella posizione specificata. Per impostazione predefinita, l'immagine viene salvata nella cartella di Librerie/Documenti, con un formato del nome dell'immagine predefinito che include:

<PRODUCT>_BMR_<Platform>_<OS Kernel>_<version>(Build xxx).ISO

Esempio:

D2D_BMR_x86x64_w8_r16.5 (Build 1234).ISO

Definire un limite per il numero di backup simultanei

L'applicazione consente di definire un limite per il numero di processi di backup di CA ARCserve D2D eseguiti simultaneamente. Questa funzionalità consente di ottimizzare le prestazioni del server proxy del computer virtuale CA ARCserve D2D nell'ambiente di backup. Per impostazione predefinita, Host-Based VM Backup è in grado di eseguire un massimo di dieci processi di backup D2D contemporaneamente In ambienti che contengono molti computer virtuali associati a un sistema proxy del computer virtuale CA ARCserve D2D, una quantità elevata di backup simultanei può compromettere le prestazioni del backup e della rete.

Nota: se la quantità di processi simultanei supera il limite definito, i processi che superano il limite inserito vengono messi in coda.

Procedere come descritto di seguito:

1. Accedere al sistema proxy del computer virtuale CA ARCserve D2D.
2. Aprire l'editor del Registro di sistema di Windows e cercare la seguente chiave:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA ARCSERVE D2D
   ```

3. Fare clic con il pulsante destro del mouse su CA ARCserve D2D e selezionare Nuovo e fare clic su Valore stringa nel menu di scelta rapida.

   Assegnare alla chiave il nome seguente:

   `VsphereMaxJobNum`

4. Fare clic su VsphereMaxJobNum, quindi su Modifica nel menu di scelta rapida.

   Viene visualizzata la finestra di dialogo di modifica della stringa.

5. Nel campo del valore dati, specificare il numero di processi di backup di CA ARCserve D2D eseguibili simultaneamente.

   - **Limite massimo -** 1
   - **Limite massimo -** nessuno.

6. Fare clic su OK. Il limite è definito.

7. Riavviare il servizio Web di CA ARCserve D2D.

Aumento della quantità di messaggi mantenuti nel file di registro VMVixMgr

Il file di registro VMVixMgr mantiene i messaggi relativi alle operazioni VMware VIX. Per ulteriori informazioni sull'API di VMware VIX, consultare il sito Web VMware.

Il file di registro VMVixMgr (VMVixMgr.log) è contenuto nella seguente directory sul sistema proxy di backup:

`C:\Program Files\CA\ARCserve D2D\Logs`

Per impostazione predefinita, il file di registro non può superare i 500 KB. Quando il file di registro supera i 500 KB, i messaggi contenuti nel file di registro verranno sovrascritti. Questo comportamento impedisce al file di registro di superare i 500 KB.

Quando viene definita una pianificazione dei dati di backup a intervalli di 15 minuti, è possibile che il file di registro venga sovrascritto se supera i 500 KB. L'aumento delle dimensioni del file di registro consente di mantenere più messaggi nel file di registro.

Si consiglia di aumentare la dimensione del file di registro soltanto quando viene definita una pianificazione per il backup dei dati ogni 15 minuti.

Procedere come descritto di seguito:

1. Collegarsi al sistema proxy di backup.

2. Aprire l'editor del Registro di sistema di Windows e cercare la seguente chiave:

   `HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA ARCserve D2D`

3. Fare clic con il pulsante destro del mouse su CA ARCserve D2D, selezionare Nuovo, quindi DWORD dal menu di scelta rapida.

   Denominare il valore DWORD nella seguente maniera:

   `VixMgrLogSize`

   Nota: se il valore DWORD non è presente, il valore predefinito del file di registro corrisponderà a 500 KB.

4. Dopo aver creato il valore DWORD, fare clic con il tasto destro del mouse su VixMgrLogSize, quindi selezionare Modifica dal menu di scelta rapida per aprire la finestra di dialogo Modifica del valore DWORD.

5. Nella finestra di dialogo Modifica del valore DWORD, specificare un valore (in KB) nel campo Dati del valore per il file di registro. Ad esempio, 750, 1000, etc.

6. Fare clic su OK per applicare il valore e chiudere la finestra di dialogo Modifica del valore DWORD.

Proteggere il proxy di backup di CA ARCserve D2D

Le sessioni di backup create con CA ARCserve Central Host-Based VM Backup sono archiviate nel proxy di backup. Sono disponibili diversi modi per proteggere il proxy di backup, a seconda della configurazione.

- Se si esegue CA ARCserve Central Protection Manager, è possibile aggiungere il proxy di backup come un nodo da proteggere. Per ulteriori informazioni, consultare la Guida per l'utente di CA ARCserve Central Protection Manager.
- Avviare l'istanza di CA ARCserve D2D in esecuzione localmente sul proxy di backup e configurare le impostazioni di backup. Selezionare l'intero computer come origine del backup. Per ulteriori informazioni, consultare la Guida per l'utente di CA ARCserve D2D.
- Se si esegue CA ARCserve Backup, è possibile configurare un processo di backup per proteggere il proxy.

Impatto del processo di installazione sui sistemi operativi

Il processo di installazione di CA ARCserve Central Applications aggiorna i vari componenti del sistema operativo Windows utilizzando un modulo di installazione denominato MSI (Microsoft Installer Package). I componenti inclusi nel file MSI consentono a CA ARCserve Central Applications di eseguire operazioni personalizzate che consentono di installare o aggiornare CA ARCserve Central Applications.

Nella tabella seguente vengono descritte le azioni personalizzate e i componenti interessati.

Nota: tutti i pacchetti MSI di CA ARCserve Central Applications richiamano i componenti elencati in questa tabella quando si installa CA ARCserve Central Applications.

Componente	Descrizione
CallAllowInstall	Consente al processo di installazione di verificare le condizioni relative all'installazione corrente dell'applicazione.
CallPreInstall	Consente al processo di installazione di eseguire la lettura e la scrittura delle proprietà del pacchetto MSI. Ad esempio, la lettura del percorso di installazione dell'applicazione dal pacchetto MSI.
CallPostInstall	Consente al processo di installazione di eseguire varie operazioni relative all'installazione. Ad esempio,la registrazione dell'applicazione nel Registro di sistema di Windows.
CallAllowUninstall	Consente al processo di disinstallazione di verificare le condizioni relative all'installazione corrente dell'applicazione.
CallPreUninstall	Consente al processo di disinstallazione di eseguire varie operazioni relative alla disinstallazione. Ad esempio, l'annullamento della registrazione dell'applicazione dal Registro di sistema di Windows.
CallPostUninstall	Consente al processo di disinstallazione di eseguire varie attività dopo la disinstallazione dei file installati. Ad esempio, la rimozione dei file restanti.
ShowMsiLog	Consente di visualizzare il file di registro di Windows Installer in Notepad se si seleziona la casella di controllo Mostra registro di Windows Installer nelle finestre di dialogo di completamento dell'installazione, di errore dell'installazione o di interruzione dell'installazione. Sarà quindi necessario fare clic su Fine. (funziona solo con Windows Installer 4.0.)
ISPrint	Stampa il contenuto di un controllo ScrollableText in una finestra di dialogo. Azione personalizzata del file .dll di Windows Installer. Il nome del file DLL è SetAllUsers.dll e il punto di ingresso è PrintScrollableText.

Componente	Descrizione
CheckForProductUpdates	Utilizza FLEXnet Connect per verificare la disponibilità di aggiornamenti di prodotto. Questa azione personalizzata avvia un file eseguibile denominato Agent.exe e trasmette la seguente istruzione: /au[ProductCode] /EndOfInstall
CheckForProductUpdatesOnReboot	Utilizza FLEXnet Connect per verificare la disponibilità di aggiornamenti di prodotto al riavvio. Questa azione personalizzata avvia un file eseguibile denominato Agent.exe e trasmette la seguente istruzione: /au[ProductCode] /EndOfInstall /Reboot

- **Directory aggiornate** - Per impostazione predefinita, il processo di installazione installa e aggiorna i file dell'applicazione nelle seguenti directory:

  `C:\Program Files\CA\`*<application name> (ad esempio, ARCserve Central Applications o ARCserve D2D)*

  È possibile installare l'applicazione nella directory di installazione predefinita oppure in una directory alternativa. Il processo di installazione copia vari file di sistema nella directory seguente:

  `C:\WINDOWS\SYSTEM32`

- **Aggiornamento delle chiavi del Registro di sistema di Windows** - Durante il processo di installazione vengono aggiornate le seguenti chiavi del Registro di sistema di windows:

  Chiavi predefinite del Registro di sistema:

  `HKLM\SOFTWARE\CA\`*<application name> (ad esempio, ARCserve Central Applications o ARCserve D2D)*

  Il processo di installazione modifica e crea nuove chiavi del Registro di sistema, in base alla configurazione del sistema in uso.

- **Applicazioni installate** - Il processo di installazione installa le seguenti applicazioni nel computer in uso:
  - CA Licensing
  - Microsoft Visual C++ 2010 SP1 Redistributable
  - Java Runtime Environment (JRE) 1.7.0_06
  - Tomcat 7.0.29

File binari con informazioni non corrette sulla versione dei file

CA ARCserve Central Applications esegue l'installazione di file binari sviluppati da terze parti, altri prodotti CA, e CA ARCserve Central Applications contenenti informazioni sulla versione dei file incorrette. La seguente tabella descrive tali file binari.

Nome file binario	Origine
UpdateData.exe	CA License
zlib1.dll	Zlib Compression Library

File binari non contenenti il manifesto integrato

CA ARCserve Central Applications installa i file binari sviluppati da terze parti, altri prodotti CA Technologies, e file CA ARCserve Central Applications non contenenti un manifesto integrato o un manifesto di testo. La seguente tabella descrive tali file binari.

Nome file binario	Source (Origine)
BaseLicInst.exe	CA License
UpdateData.exe	CA License
vcredist_x64.exe	Microsoft
vcredist_x86.exe	Microsoft
tomcat7.exe	Tomcat

File binari che richiedono un livello di privilegi di tipo Amministratore nel manifesto

CA ARCserve Central Applications installa file binari sviluppati da terze parti, da altri prodotti CA Technologies e file CA ARCserve Central Applications che richiedono un livello di privilegi di tipo Amministratore o più elevato. Per poter eseguire i servizi, i componenti e le applicazioni di CA ARCserve Central Applications è necessario effettuare l'accesso utilizzando un account amministrativo o un account che dispone di autorizzazioni più elevate. I file binari corrispondenti a tali servizi, componenti e applicazioni includono funzionalità specifiche di CA ARCserve Central Applications non disponibili per un account utente di base. Ne consegue che per completare un'operazione in Windows verrà richiesto di confermare tale operazione mediante l'immissione di una password oppure mediante l'utilizzo di un account che dispone di privilegi di amministrazione.

- **Privilegi di amministratore:** un profilo o un account amministrativo con privilegi di amministratore dispongono di autorizzazioni di lettura, scrittura ed esecuzione per tutte le risorse di sistema e di Windows. Se non si dispone di privilegi di amministratore, verrà richiesto di immettere il nome utente e la password di un utente con tali privilegi per poter continuare.
- **Privilegi più elevati disponibili:** un account con i privilegi più elevati disponibili consiste in un account utente di base e in un account utente avanzato eseguiti con privilegi di amministratore.

La seguente tabella descrive tali file binari.

Nome file binario	Origine
APMSetupUtility.exe	CA ARCserve Central Applications
ArcAppUpdateManager.exe	CA ARCserve Central Applications
CA ARCserve Central ApplicationsAutoUpdateUninstallUtility.exe	CA ARCserve Central Applications
CA ARCserve Central ApplicationsPMConfigSettings.exe	CA ARCserve Central Applications
CCIConfigSettings.exe	CA ARCserve Central Applications
CfgUpdateUtil.exe	CA ARCserve Central Applications
CfgUpdateUtil.exe	CA ARCserve Central Applications
D2DAutoUpdateUninstallUtility.exe	CA ARCserve Central Applications
D2DPMConfigSettings.exe	CA ARCserve Central Applications
D2DUpdateManager.exe	CA ARCserve Central Applications
DBConfig.exe	CA ARCserve Central Applications
FWConfig.exe	CA ARCserve Central Applications

Nome file binario	Origine
RemoteDeploy.exe	CA ARCserve Central Applications
RestartHost.exe	CA ARCserve Central Applications
SetupComm.exe	CA ARCserve Central Applications
SetupFW.exe	CA ARCserve Central Applications
SetupWrapper.exe	CA ARCserve Central Applications
Uninstall.exe	CA ARCserve Central Applications
UpdateInstallCommander.exe	CA ARCserve Central Applications
UpgradeDataSyncupUtility.exe	CA ARCserve Central Applications
jbroker.exe	Java Runtime Environment
jucheck.exe	Java Runtime Environment

Esclusione di file dalla scansione antivirus

Il software antivirus può compromettere la corretta esecuzione di dell'applicazione bloccando temporaneamente l'accesso ai file o mettendo in quarantena ed eliminando i file classificati erroneamente come sospetti o pericolosi. È possibile configurare la maggior parte dei software antivirus per escludere determinati processi, file o cartelle affinché non venga eseguita l'analisi di dati che non necessitano di protezione. La corretta configurazione del software antivirus è fondamentale per evitare che interferisca con le operazioni di backup e ripristino o con qualsiasi altro processo.

I seguenti processi, cartelle e file dovranno essere esclusi dall'analisi anti-virus:

- Elenco di processi
  - C:\Programmi\CA\ARCserve Central Applications\BIN\CCIConfigSettings.exe
  - C:\:\Programmi\CA\ARCserve Central Applications\BIN\CfgUpdateUtil.exe
  - C:\Programmi\CA\ARCserve Central Applications\BIN\DBConfig.exe
  - C:\Programmi\CA\ARCserve Central Applications\BIN\GetApplicationDetails.exe
  - C:\Programmi\CA\ARCserve Central Applications\BIN\GetApplicationDetails64.exe
  - C:\Programmi\CA\ARCserve Central Applications\BIN\GetVolumeDetails.exe
  - C:\Programmi\CA\ARCserve Central Applications\BIN\VixGetApplicationDetails.exe
  - C:\Programmi\CA\ARCserve Central Applications\BIN\VixGetVolumeDetails.exe
  - C:\Programmi\CA\ARCserve Central Applications\BIN\GetApplicationDetails64.exe
  - C:\Programmi\CA\ARCserve Central Applications\Deployment\Asremsvc.exe
  - C:\Programmi\CA\ARCserve Central Applications\Deployment\CheckProdInfo.exe
  - C:\Programmi\CA\ARCserve Central Applications\Deployment\DeleteMe.exe
  - C:\Programmi\CA\ARCserve Central Applications\Deployment\SetupComm.exe
  - C:\Programmi\CA\ARCserve Central Applications\Deployment\RestartHost.exe
  - C:\Programmi\CA\ARCserve Central Applications\Update Manager\D2DAutoUpdateUninstallUtility.exe
  - C:\Programmi\CA\ARCserve Central Applications\Update Manager\D2DPMConfigSettings.exe
  - C:\Programmi\CA\ARCserve Central Applications\Update Manager\D2DUpdateManager.exe
  - C:\Programmi\CA\ARCserve Central Applications\Update Manager\UpgradeDataSyncupUtility.exe

- C:\Programmi\CA\ARCserve Central Applications\TOMCAT\BIN\tomcat7.exe
- C:\Programmi\CA\ARCserve D2D\TOMCAT\JRE\jre7\bin
  - java.exe
  - java-rmi.exe
  - javaw.exe
  - keytool.exe
  - rmid.exe
  - rmiregistry.exe
- C:\Programmi(x86)\CA\SharedComponents\CA_LIC
  - CALicnse.exe
  - CAminfo.exe
  - CAregit.exe
  - ErrBox.exe
  - lic98log.exe
  - lic98Service.exe
  - lic98version.exe
  - LicDebug.exe
  - LicRCmd.exe
  - LogWatNT.exe
  - mergecalic.exe
  - mergeolf.exe

Glossario

Criterio

Un criterio è un insieme di specifiche per la protezione di un nodo in uno o più CA ARCserve Central Applications.

File catalogo

Un file di catalogo è una directory di informazioni sui dati di backup contenuti nel database di CA ARCserve D2D. Per ulteriori informazioni sul file di catalogo di CA ARCserve D2D, consultare la *Guida per l'utente di CA ARCserve D2D.*

Gruppo nodo

Un gruppo nodo è un metodo in base al quale tutti i nodi gestiti da uno o più CA ARCserve Central Applications possono essere organizzati, ad esempio in base allo scopo, al sistema operativo o alle applicazioni installate.

Modalità di trasporto HOTADD

La modalità di trasporto HOTADD è un metodo di trasporto dei dati che consente di eseguire il backup dei computer virtuali configurati con dischi SCSI. Per ulteriori informazioni, consultare la guida alla programmazione Virtual Disk API Programming Guide disponibile sulla pagina Web di VMware.

Modalità di trasporto NBD

La modalità di trasporto Network Block Device (NBD), denominata anche modalità di trasporto LAN, utilizza il protocollo NFC (Network File Copy) per la comunicazione. Diverse operazioni VDDK e VCB utilizzano una connessione per ciascun disco virtuale a cui effettuano l'accesso su ciascun server host ESX/ESXi, durante l'utilizzo di NDB.

Modalità di trasporto NBDSSL

La modalità di trasporto NBDSSL (Network Block Device Secure Sockets Layer) utilizza il protocollo di comunicazione NFC (Network File Copy). NBDSSL esegue il trasferimento dei dati crittografati mediante le reti di comunicazione TCP/IP.

Modalità di trasporto SAN

La modalità di trasporto SAN (Storage Area Network) consente il trasferimento dei dati di backup da sistemi proxy connessi alla rete SAN a periferiche di archiviazione mediante la comunicazione Fibre Channel.

Nodo

Un nodo è un computer fisico o virtuale gestito da uno o più CA ARCserve Central Applications.

Proxy di backup

Un backup di proxy è il computer host in cui CA ARCserve D2D è in esecuzione. Il proxy esegue le operazioni di backup configurate in CA ARCserve Central Host-Based VM Backup.

Punto di ripristino

Un punto di ripristino è un'immagine di backup costituita da blocchi parent-plus-oldest-child. I backup secondari sono uniti ai backup principali per creare nuove immagini di punto di ripristino in modo che il valore specificato sia sempre aggiornato.

Rilevamento automatico

Il rilevamento automatico è un processo in base al quale i nodi sono rilevati e aggiunti a uno o più CA ARCserve Central Applications per la gestione centralizzata.

Sincronizzazione

La sincronizzazione è il processo in base al quale i dati in database diversi vengono mantenuti aggiornati in modo che il database del sito centrale sia coerente con i rami, i nodi o i siti registrati.

SRM

La Gestione delle risorse di archiviazione (SRM) è una funzionalità in base alla quale le informazioni vengono raccolte per una gestione efficacie dell'ambiente, ad esempio dati su applicazioni, hardware e software o gli indicatori di prestazioni chiave.

Verifica preliminare

L'utilità di verifica preliminare consente di eseguire controlli importanti sui nodi per rilevare condizioni che potrebbero impedire la corretta esecuzione dei processi di backup. È possibile visualizzare i risultati della verifica preliminare di un nodo selezionando l'icona nella colonna Stato della verifica preliminare nella schermata Nodo.